Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)

TRA-1

Date : le 23 octobre 2007

Page intentionnellement laissée en blanc

Avant-propos

La *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)* est une publication non classifiée, publiée sous l'autorité du chef du Centre de la sécurité des télécommunications (CST) et du Commissaire de la Gendarmerie royale du Canada (GRC). Elle remplace ou redéfinit les publications du CST et de la GRC suivantes :

- ITSG-04, *Guide de travail pour l'évaluation des menaces et des risques*;
- G2-001, *Guide d'évaluation de la menace et des risques pour les technologies de l'information*;
- R1-001, *Évaluation de la menace et des risques impliquant un examen sur place de la sécurité matérielle*;
- R1-001a/b, *Éléments de base de l'EMR*;
- R1-001c, *Énoncé de sensibilité de l'EMR*; et
- R1-003, *Notes/formulaire d'enquête*.

Cette version initiale de la *Méthodologie harmonisée d'EMR* doit être considérée comme une version intérimaire d'ici à ce que soit terminé le projet de renouvellement de l'ensemble des politiques du Secrétariat du Conseil du Trésor. Elle devra être mise à jour une fois que la *Politique du gouvernement sur la sécurité* et les normes connexes auront été révisées et remplacées. Ceci étant dit, la mécanique réelle de la méthodologie demeurera probablement inchangée; seuls les renvois aux politiques, directives et normes supérieures sont susceptibles de changer de manière significative.

Toute suggestion de modification et demande de clarification doit être acheminée par les voies ministérielles sécurisées à votre représentant des Services à la clientèle du CST ou à la Sous-direction de la sécurité technique de la GRC.

Pour des conseils et directives concernant la *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)*, communiquez avec les organismes suivants :

Services à la clientèle des services de TI
Centre de la sécurité des télécommunications
C.P. 9703, Terminus
Ottawa (Ontario) K1G 3Z4
Téléphone : 613-991-7600
Courrier électronique : client.svcs@cse-cst.gc.ca

Gendarmerie royale du Canada
Sous-direction de la sécurité technique
Courrier électronique : traclientservices@rcmp-tsb.ca

Des options de formation particulières sont décrites dans les sites Web suivants :

Centre de la sécurité des télécommunications
http://www.cse-cst.gc.ca/training/training-f.html

Gendarmerie royale du Canada
http://www.rcmp-grc.gc.ca/tsb/workshops/index_f.htm

Date d'entrée en vigueur

Cette publication entre en vigueur le 28 août 2007

Gwen Beauchemin
Directrice, Gestion de la mission de la Sécurité des TI
Centre de la sécurité des télécommunications

Guylaine Dansereau
Directrice, Sous-direction de la sécurité technique
Gendarmerie royale du Canada

© 2007 Gouvernement du Canada, Centre de la sécurité des télécommunications / Gendarmerie royale du Canada

Il est interdit de copier cette publication, en tout ou en partie, sans l'autorisation écrite du CST ou de la GRC.

Historique des révisions

Document n^{o}	Titre	Date de diffusion

Page intentionnellement laissée en blanc

Table des matières

Avant-propos i
Historique des révisions iii
Table des matières v
Liste des tableaux vii
Liste des figures ix
Introduction IN-1
Aperçu général AG-1
Sommaire de gestion SG-1
Annexe A - Phase de préparation A-1
Appendice A-1 – Les EMR dans un plan de projet/cycle de vie d'un système A1-1
Appendice A-2 - Normes de sécurité et évaluations des menaces et des risques A2-1
Appendice A-3 - Composition de l'équipe d'EMR A3-1
Appendice A-4 - Recours à des consultants en EMR A4-1
Appendice A-5 - Exemple d'énoncé des travaux pour services de consultants en EMR A5-1
Appendice A-6 - Exemple de plan de travail d'EMR A6-1
Annexe B - Phase d'identification et d'évaluation des biens B-1
Appendice B-1 - Sources de données sur les biens B1-1
Appendice B-2 - Liste des biens B2-1
Appendice B-3 - ARO, EFVP et EMR B3-1
Appendice B-4 - Tableau détaillé des préjudices B4-1
Appendice B-5 - Tableau d'évaluation des biens / Énoncé de sensibilité B5-1
Annexe C - Phase d'évaluation des menaces C-1
Appendice C-1 - Sources de données sur les menaces C1-1
Appendice C-2 – Liste des menaces C2-1
Appendice C-3 - Paramètres des menaces C3-1
Appendice C-4 - Tableau d'évaluation des menaces C4-1
Annexe D – Évaluation des vulnérabilités D-1
Appendice D-1 - Sources de données sur les vulnérabilités D1-1
Appendice D-2 - Liste des vulnérabilités D2-1
Appendice D-3 - Paramètres des vulnérabilités D3-1
Appendice D-4 - Tableau d'évaluation des vulnérabilités D4-1
Annexe E - Calcul des risques résiduels E-1
Appendice E-1 - Tableaux des risques résiduels E1-1
Appendice E-2 – Liste des risques résiduels évalués E2-1

Annexe F – Phase des recommandations F-1
Appendice F-1 - Sources de données sur les mesures de protection F1-1
Appendice F-2 – Liste des mesures de protection F2-1
Appendice F-3 – Sélection des mesures de protection potentielles F3-1
Appendice F-4 – Calcul de la rentabilité des mesures de protection F4-1
Appendice F-5 – Tableau des recommandations F5-1
Appendice F-6 – Plan du rapport d'EMR F6-1
Appendice F-7 – Exemple de rapport d'EMR F7-1

Annexe G - Conclusion G-1
Appendice G-1 – Feuille de travail EMR G1-1
Appendice G-2 – Glossaire et acronymes G2-1
Appendice G-3 – Documents de référence G3-1

Liste des tableaux

Tableau A-1: Longueur type des rapports d'EMR A-9
Tableau A1-1 : Stades relatifs à un plan de projet ou à un cycle de vie d'un système..... A1-3
Tableau A6-1 : Composition de l'équipe chargée de l'EMR A6-3
Tableau A6-2 : Liste simple des activités de l'EMR..... A6-6
Tableau B-1 : Catégorisation des biens selon les degrés de préjudice indiqués dans la PGS B-7
Tableau B-2 : Valeurs comparatives des biens..... B2-9
Tableau B-3 : Tableau abrégé des préjudices et des valeurs des biens B3-10
Tableau B-4 : Exemple de tableau d'évaluation des biens/énoncé de sensibilité..... B4-17
Tableau B3-1: Processus comparatif - mise en correspondance : ARO, EFVP et EMR..... B3-6
Tableau C-1: Tableau des probabilités des menaces C-14
Tableau C-2 : Tableau de la gravité des menaces..... C-16
Tableau C-3 : Tableau des niveaux de menace..... C-17
Tableau C-4 : Exemple de tableau d'évaluation des menaces..... C-20
Tableau C3-1 : Tableau des probabilités des menaces C3-2
Tableau C3-2 : Tableau de la gravité des menaces..... C3-2
Tableau C3-3 : Tableau des niveaux de menace..... C3-3
Tableau D-1 : Tableau des incidences des mesures de protection..... D-6
Tableau D-2 : Incidence des vulnérabilités sur la probabilité de compromission (prévention)D-17
Tableau D-3 : Incidence-vulnérabilités - gravité-conséquences (détection, réaction, reprise). .. D-19
Tableau D-4 : Évaluation de base des vulnérabilités..... D-20
Tableau D-5 : Exemple de tableau d'évaluation des vulnérabilités D-23
Tableau D3-1 : Incidence des vulnérabilités - probabilité de compromission (prévention)..... D3-1
Tableau D3-2 : Incidence-vulnérabilités - gravité-conséquences (détection, réaction, reprise) D3-2
Tableau D3-3 : Évaluation de base des vulnérabilités..... D3-2
Tableau E-1 : Cotes numériques - Niveaux - valeur : bien, menaces et vulnérabilités E-2
Tableau E-2 : Niveaux et gammes de risques.....E-3
Tableau E-3: Liste des risques résiduels évalués.....E-5

Tableau E1-1 : Cotes numériques - Niveaux – valeur : bien, menaces et vulnérabilités E1-2
Tableau E1-2 : Niveaux et gammes de risques.....E1-2
Tableau E1-3: Tableau des risques pour les valeurs de bien très faibles.....E1-2
Tableau E1-4 : Tableau des risques pour les valeurs de bien faibles E1-3
Tableau E1-5: Tableau des risques pour les valeurs de bien moyennes.....E1-3
Tableau E1-6: Tableau des risques pour les valeurs de bien élevées E1-3
Tableau E1-7: Tableau des risques pour les valeurs de bien très élevées E1-3
Tableau F-1 : Acceptabilité des risques résiduels évalués.....F-3
Tableau F3-1 : Liste abrégée des risques résiduels évalués F3-2
Tableau F3-2 : Liste des risques résiduels évalués inacceptables F3-4
Tableau F3-3 : Liste des mesures de protection potentielles.....F3-7
Tableau F3-4 : Risques résiduels projetés - Entrée verrouillée et accès avec escorte.....F3-9
Tableau F3-5 : Risques résiduels projetés - Ajout d'un avertisseur individuel et d'un gardien de sécurité sur appel F3-10
Tableau F3-6 : Risques résiduels projetés - Gardien de sécurité, etc. F3-11
Tableau F4-1 : Coûts initiaux et récurrents directs et indirects.....F4-4
Tableau F4-2 : Calcul de la rentabilité des mesures de protection.....F4-5
Tableau F7-1 : Calcul du risque résiduel évalué.....F7-3

Liste des figures

Figure IN-1 : Structure modulaire de la méthodologie harmonisée d'EMR IN-5
Figure AG-1: Processus de gestion intégrée du risque AG-1
Figure AG-2: Cadre de responsabilisation de gestion AG-2
Figure AG-3: Méthodologie harmonisée d'EMR - appui de fonction moderne de contrôleur AG-4
Figure SG-1 : Cadre contextuel de la méthodologie harmonisée d'EMR SG-2
Figure SG-2 : Phases et processus d'un projet d'EMR SG-3
Figure SG-3 : Modèle (très) simplifié de gestion des risques SG-10
Figure A1-1: Flux d'information d'EMR dans un environnement de projet A1-5
Figure A2-1: Méthodologies de gestion des risques A2-3
Figure A2-2: Structure des documents sur la sécurité A2-5
Figure A4-1 : Embauche de consultants pour accroître le personnel dédié aux EMR A4-3
Figure A6-1 : Diagramme illustrant les projets d'EMR interreliés pour une seule installation A6-2
Figure B-1 : Modèle d'identification des biens B-4
Figure B-2 : Exemple d'un segment de la structure hiérarchique de la liste des biens B-5
Figure B-3 : Sélection des biens inclus dans la portée d'un projet d'EMR B-6
Figure B-4 : Valeurs des biens fondées sur une compromission totale B-11
Figure B3-1: Portée d'une EMR B3-2
Figure B3-2: Portée d'une ARO B3-3
Figure B3-3: Portée d'une EFVP B3-3
Figure C-1 : Modèle général de menace C-3
Figure C-2 : Exemple de segment de la structure hiérarchique de la liste des menaces C-5
Figure C-3 : Menaces directes et indirectes C-11
Figure D-2 : Structure hiérarchique de la liste des vulnérabilités D-13
Figure E-1 : Calcul du risque résiduel E-2
Figure F-1 : Stratégie de sécurité active F-6
Figure F-2 : Calcul du coût annuel amorti F-13
Figure F-3 : Calcul de la rentabilité des mesures de protection F-14

Page intentionnellement laissée en blanc

Introduction

1 Contexte

> « Les ministères sont tenus de satisfaire aux exigences suivantes : […]
> − Appliquer les mesures de protection de sécurité matérielle et des technologies de l'information aux renseignements et aux biens de nature délicate selon les normes [et les évaluations de la menace et des risques.] »
>
> *Politique du gouvernement sur la sécurité*, juin 1986

Lorsque la première *Politique du gouvernement sur la sécurité (PGS)* été adoptée en juin 1986, elle instaurait plusieurs concepts importants, dont la protection de l'information et des biens sensibles en fonction de normes de sécurité minimales et d'une évaluation des menaces et des risques connexes. Peu après, le processus d'évaluation des menaces et des risques (EMR) était décrit plus en détail à la section 9 de la *Norme de sécurité relative à l'organisation et l'administration*. Néanmoins, il était évident que les institutions gouvernementales auraient besoin d'instructions et de directives plus précises encore sur la réalisation des EMR avant de pouvoir elles-mêmes en faire. Par conséquent, au cours des quinze années qui ont suivi, deux organismes investis de responsabilités précises en matière de prestation de conseils sur les EMR aux termes de l'appendice A de la politique, à savoir le Centre de la sécurité des télécommunications (CST) et la Gendarmerie royale du Canada (GRC), ont publié une série de documents techniques, dont les suivants :

- *Guide pour la préparation d'un énoncé de sécurité matérielle* (G1-005);
- *Guide d'évaluation de la menace et des risques impliquant un examen sur place de la sécurité matérielle*;
- *Guide d'évaluation de la menace et des risques pour les technologies de l'information (TI)* (G2-001);
- *Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information* (MG-2);
- *Guide d'évaluation des risques et de sélection des mesures de protection pour les technologies de l'information* (MG-3);
- *Guide de certification et d'accréditation des technologies de l'information* (MG-4);
- *Guide de travail pour l'évaluation des menaces et des risques* (ITSG-04).

2 Problèmes

> « Des 82 ministères et organismes qui faisaient partie de notre enquête, seulement 37 (soit 45 p. 100) avaient effectué, conformément à la Politique et aux normes, une évaluation des menaces et des risques pesant sur leurs programmes, systèmes et services. »
>
> *Vérification de la sécurité des technologies de l'information*, février 2005

Malgré ces efforts constants pour élaborer des instructions explicites sur la préparation des EMR, de nombreuses institutions gouvernementales ont eu des difficultés considérables avec le processus, qui était souvent considéré comme inutilement complexe et inflexible. Ces problèmes étaient aggravés par le fait que les organismes responsables

avaient, dans la pratique, élaboré trois méthodologies d'EMR différentes, une pour la sécurité matérielle et deux autres pour les systèmes de TI. Bien que les principes fondamentaux soient restés les mêmes, les nombreuses différences entre les diverses lignes directrices et la formation connexe ont entraîné une certaine confusion et des incohérences dans leur application. En fait, la vérificatrice générale a constaté ces incohérences ainsi qu'une réticence généralisée à effectuer des EMR dans sa vérification de la sécurité des technologies de l'information de février 2005.

3 Objectifs

Afin de répondre à ces préoccupations légitimes et de favoriser l'utilisation des EMR, le CST et la GRC ont entrepris un projet conjoint en décembre 2004 en vue d'élaborer une seule méthodologie harmonisée d'évaluation des menaces et des risques pour le gouvernement du Canada dont les buts ou objectifs sont les suivants :

- **Flexibilité.** La nouvelle méthodologie doit être **extensible** pour pouvoir être appliquée à tous les biens, matériels et de TI, grands et petits, suffisamment en détail pour satisfaire aux objectifs opérationnels. Elle doit soutenir différents niveaux de **granularité** ainsi qu'une capacité de synthèse, des analyses très détaillées ou ciblées aux survols plus généraux, dépendant de l'environnement de risque et de l'objet de l'évaluation.
- **Modularité.** Afin de permettre la décomposition d'EMR plus grosses et plus complexes en composants plus petits et plus maniables, la nouvelle méthodologie doit soutenir une analyse modulaire au moyen de liens adéquats entre les éléments connexes.
- **Simplicité.** La logique qui sous-tend la méthodologie doit être satisfaisante intuitivement et énoncée simplement afin que les gestionnaires de programmes et de projets ainsi que les spécialistes de la sécurité puissent la suivre facilement. Pour accroître la convivialité, il faut illustrer les principes et processus fondamentaux de la méthodologie harmonisée au moyen de graphiques, diagrammes, exemples, tableaux et modèles détaillés.
- **Cohérence.** Pour que les EMR effectuées par les différents organismes soient plus cohérentes, la nouvelle méthodologie doit établir un vocabulaire commun et des définitions simples pour tous les aspects de la gestion des risques. De solides paramètres pour les variables de risque, plus précisément la valeur des biens, les menaces et les vulnérabilités, sont indispensables à une analyse comparative et des résultats reproduisables, éléments essentiels à une communication éclairée des risques, une interopérabilité améliorée et des solutions de sécurité rentables.
- **Application générale.** La méthodologie doit s'appliquer de la même façon aux biens matériels et aux biens de TI, ainsi qu'à la protection des employés et à la prestation des services.
- **Automatisation.** La méthodologie harmonisée d'évaluation des menaces et des risques est un outil manuel, mais elle a été élaborée dans une optique d'automatisation afin de soutenir et de simplifier davantage le processus d'EMR.

4 Principes

Certains principes importants ont guidé l'élaboration de la méthodologie harmonisée d'évaluation des menaces et des risques, dont les suivants :

- **Compatibilité.** La nouvelle méthodologie doit mettre à profit et soutenir la PGS et les normes opérationnelles de sécurité pertinentes, particulièrement celles qui ont trait à l'identification des biens, à la gestion des risques de sécurité, à la gestion de la sécurité des technologies de l'information, à la sécurité matérielle et à la planification de la continuité des activités. Elle doit être étroitement intégrée aux politiques connexes, particulièrement celles qui ont trait à la gestion des risques, à l'accès à l'information et à la protection des renseignements personnels, ainsi qu'au Cadre de gestion intégrée du risque et au Cadre de responsabilisation de gestion.
- **Transparence.** Pour mieux répondre aux besoins des gestionnaires du gouvernement qui utiliseront la nouvelle méthodologie en fin de compte, de vastes consultations interministérielles ainsi que des séances d'information régulières et un groupe de discussion actif composé d'utilisateurs ont été organisés pendant le processus d'élaboration.
- **Changements évolutifs.** Au cours des vingt dernières années, les organismes responsables de la sécurité ont investi beaucoup de temps et d'efforts pour élaborer les diverses méthodologies d'EMR ainsi que les lignes directrices et programmes de formation connexes. De nombreux ministères ont fait des efforts considérables pour adopter et utiliser ces outils. C'est pourquoi, afin de profiter de ces connaissances et de ces expériences, la méthodologie harmonisée d'évaluation des menaces et des risques a été élaborée en tant qu'amélioration graduelle plutôt que changement radical par rapport aux pratiques établies.

5 Structure et utilisation

Afin d'atteindre le double objectif de la simplicité et de la flexibilité à l'intérieur d'un outil tout usage exhaustif, la méthodologie harmonisée d'évaluation des menaces et des risques a été structurée de façon très modulaire et suivant plusieurs niveaux de détail, allant des sommaires de haut niveau à des descriptions de plus en plus précises de processus et de paramètres spécifiques. La plupart des segments sont limités à quelques pages, afin que les utilisateurs puissent se concentrer rapidement sur les aspects de préoccupation ou d'intérêt immédiat sans avoir à chercher dans un long exposé. Cette structure facilite également les renvois pour une accessibilité facile.

Les principaux modules de la *Méthodologie harmonisée d'évaluation des menaces et des risques* sont les suivants :

- l'**avant-propos** précisant les documents en vertu desquels la méthodologie est publiée et fournissant les coordonnées du service à qui adresser les questions et les propositions d'améliorations, en plus des habituelles table des matières et listes des figures et des tableaux;

- l'**aperçu général** expliquant l'importance des EMR en tant qu'outils pour aider les cadres supérieurs à s'acquitter de leurs responsabilités et de leurs obligations de rendre compte conformément à la fonction moderne de contrôleur et aux cadres de gestion intégrée du risque et de responsabilisation de gestion;
- l'**introduction** faisant le point sur le contexte, la raison d'être de la nouvelle méthodologie, les objectifs et principes qui ont guidé son élaboration ainsi que la structure adoptée pour atteindre ces objectifs;
- le **sommaire de gestion** décrivant tout le processus d'EMR à un niveau élevé pour les gestionnaires de programmes et de projets investis de responsabilités de gestion des risques;
- une série de six **annexes** présentant chacune une phase du processus d'EMR plus en détail pour les employés des programmes, des projets et de la sécurité qui doivent appliquer concrètement la méthodologie;
- une grande quantité d'**appendices** contenant des données plus détaillées encore sous forme de diagrammes, de descriptions techniques, de listes de contrôle, d'organigrammes, de tableaux et de modèles afin d'illustrer chacun des aspects du processus d'EMR et de faciliter une application facile;
- une septième **annexe** contenant d'autres documents à l'appui, comme un glossaire exhaustif, une liste des acronymes et des documents de référence.

Cette structure est illustrée dans la figure IN-1.

Quiconque aborde le document pour la première fois doit parcourir l'introduction (5 pages) et lire le sommaire de gestion (10 pages) très attentivement pour comprendre l'ensemble du processus. Les annexes et appendices plus détaillés visent à aider les employés des programmes ou des projets et les spécialistes de la sécurité qui sont concrètement chargés de préparer un rapport d'EMR. Il faut étudier chacun de ces documents sous tous les angles avant de commencer les phases successives d'un projet d'EMR. De nombreuses questions et préoccupations normales trouveront des réponses précises dans le corps de ces segments, souvent avec des exemples pratiques illustrant différentes solutions.

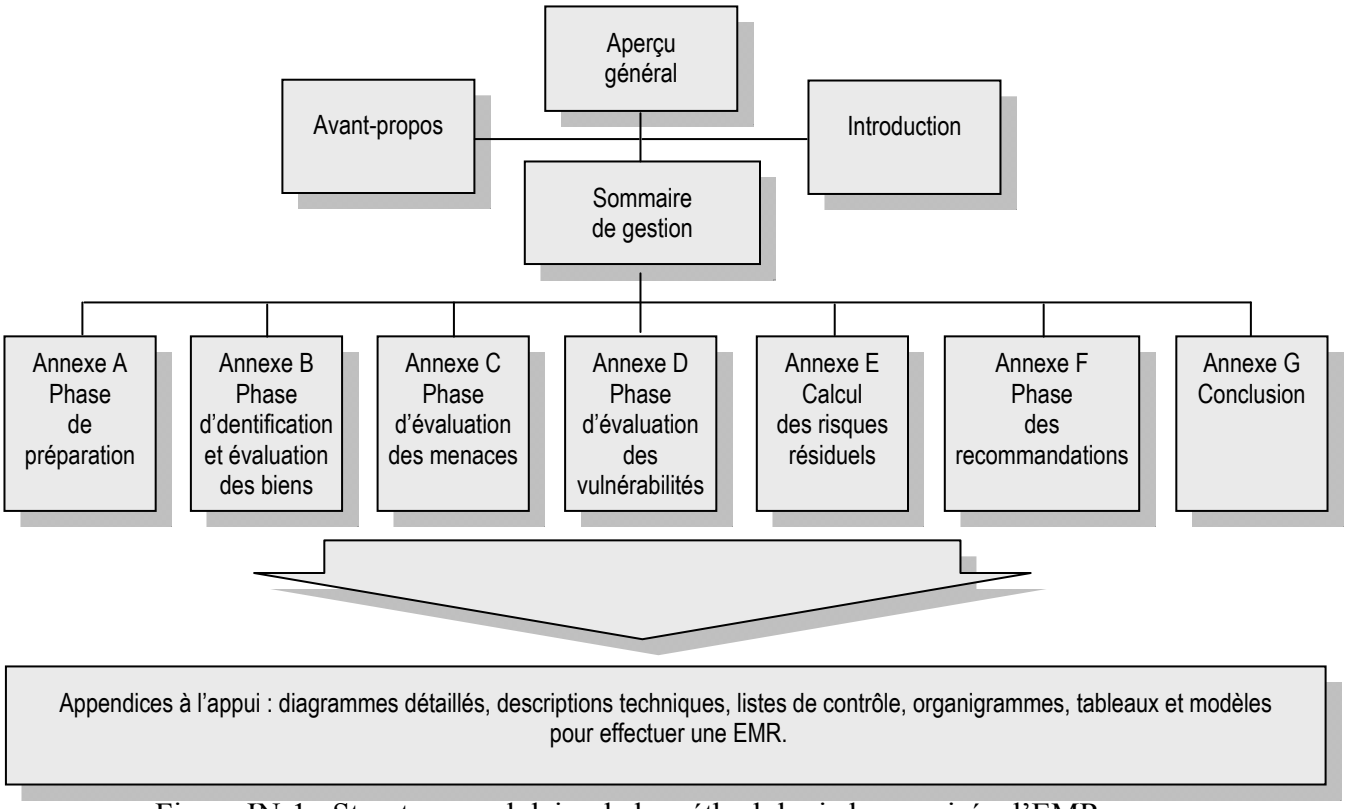

Figure IN-1 : Structure modulaire de la méthodologie harmonisée d'EMR

En plus de cette trousse exhaustive, la méthodologie harmonisée d'évaluation des menaces et des risques comprend des produits structurés de formation et de sensibilisation visant à rendre les EMR faciles d'accès et plus utiles pour les gestionnaires des risques ministériels. Ces produits comprennent :

- un programme de formation officiel accompagné d'exercices pratiques, expliquant le guide de l'utilisateur et renforçant l'expérience d'apprentissage;
- des notes d'information complémentaires pour les hauts gestionnaires de programmes et de projets, situant la méthodologie à l'intérieur du Cadre de gestion intégrée du risque dans son ensemble et de la fonction moderne de contrôleur en général.

Comme il est indiqué dans l'avant-propos, les gestionnaires des programmes et projets ministériels peuvent obtenir aide et conseils sur la méthodologie harmonisée d'évaluation des menaces et des risques et son application auprès de leur agent de sécurité du ministère et de leur coordonnateur des TI, ainsi que des organismes responsables de la sécurité, à savoir le Centre de la sécurité de télécommunications et la Gendarmerie royale du Canada.

Page intentionnellement laissée en blanc

Aperçu général

Dans le cadre de l'initiative de la **fonction moderne de contrôleur**, le document *Des résultats pour les Canadiens et les Canadiennes : Un cadre de gestion pour le gouvernement du Canada* a défini quatre engagements majeurs visant à améliorer les pratiques de gestion et à rehausser la qualité de la prestation des services : (1) accent **sur les citoyens**, (2) ensemble de **valeurs** claires, (3) gestion axée sur les **résultats** et (4) **dépenses judicieuses** étant donné la rareté des fonds publics.

De toute évidence, les nouvelles technologies offrent de nombreuses occasions de mettre au point des solutions novatrices pour relever ces défis importants, malgré les risques dus au rythme rapide de changement, à la complexité inhérente de plusieurs secteurs de service et à la variété des dangers, allant des pannes de système à l'usage abusif délibéré et aux catastrophes naturelles. La **gestion évoluée des risques**, l'un des quatre piliers de la fonction moderne de contrôleur, permet d'établir plus efficacement l'équilibre entre ces risques et ces occasions.

Le **cadre de gestion intégrée du risque,** élaboré suite au *rapport du Groupe de travail des SMA sur la gestion du risque : Gestion du risque pour le Canada et les Canadiens*, renforce la précédente *Politique sur la gestion des risques* qui exige des ministères qu'ils : (1) définissent les périls, (2) analysent et évaluent les risques et (3) mettent en œuvre des mesures économiques de contrôle des risques afin de prévenir, réduire ou les éviter. Le modèle plus détaillé en neuf étapes du cadre de gestion intégrée du risque est illustré dans la figure AG-1.

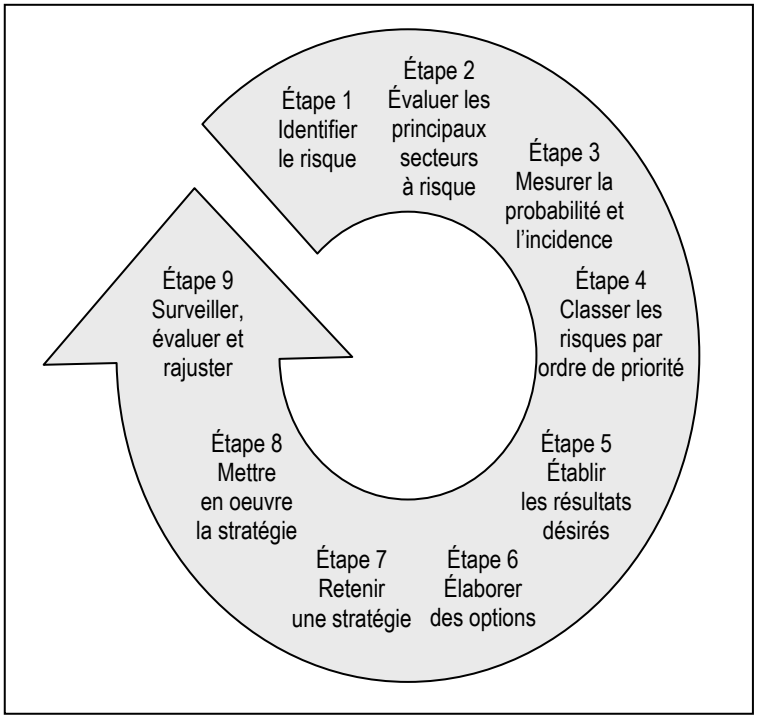

Figure AG-1: Processus de gestion intégrée du risque

Pour aider les administrateurs généraux et tous les gestionnaires de la fonction publique à évaluer le rendement organisationnel et définir les priorités pour l'amélioration de la gestion, le Secrétariat du Conseil du Trésor a élaboré un *cadre de responsabilisation de gestion* composé de 10 éléments essentiels à la saine gestion, illustrés dans la figure AG-2, incluant une série d'indicateurs et de mesure connexes d'efficacité. Bien que les dix facteurs soient intimement intégrés et entièrement interdépendants, les objectifs ultimes de **résultats et de rendement** de la prestation de **services axés sur les citoyens** ne peuvent être atteints de manière transparente, avec pleine **responsabilisation** d'une saine **gérance,** en l'absence d'une **gestion efficace des risques**. Il est également important d'assurer l'équilibre entre les occasions et les risques inhérents **à** l'**innovation et à la gestion du changement** dans un **cadre de régie** solide à l'appui d'**orientations stratégiques** conformes **aux politiques et aux programmes approuvés**. Bref, une gestion des risques éclairée est essentielle à la prise de décisions responsables.

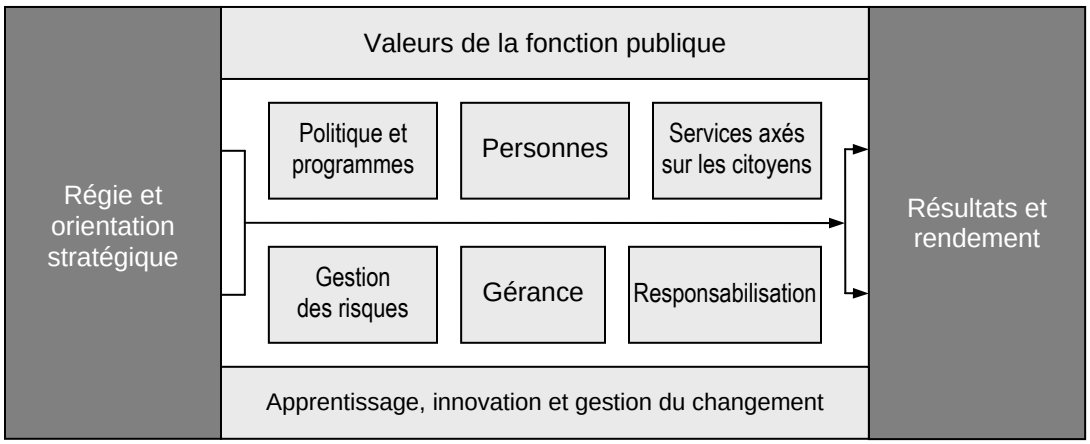

Figure AG-2: Cadre de responsabilisation de gestion

Les objectifs énoncés dans la *Politique du gouvernement sur la sécurité* (PGS) sont très similaires : « Soutenir l'intérêt national et les objectifs opérationnels du Gouvernement du Canada en assurant la sauvegarde des employés et des biens, ainsi que la prestation continue des services. » Du point de vue pratique, pour assurer la protection adéquate des employés, des biens et des services menacés, la PGS prescrit deux mécanismes complémentaires : des exigences de base en matière de sécurité et la gestion continue des risques fondée sur l'évaluation des menaces et des risques (EMR).

La dernière approche, l'EMR, est un outil particulièrement puissant qui aide les gestionnaires de programme et de projet à s'acquitter de leurs responsabilités en matière de diligence raisonnable et de saine gérance tout en cherchant des solutions novatrices pour améliorer les résultats et le rendement de la prestation des services. Plus particulièrement, la *Méthodologie harmonisée d'évaluation des menaces et des risques pour le gouvernement du Canada* propose :

- un **vocabulaire commun** pour favoriser une meilleure compréhension, des discussions plus éclairées et, par conséquent, de meilleures communications concernant la dynamique des risques;
- une **trousse d'outils souple** pour aider les gestionnaires à identifier au niveau de détail approprié les biens et les services importants ainsi que les vulnérabilités qui les exposent à des dangers potentiels;
- des **paramètres explicites** aux fins d'analyse comparative pour prioriser les risques relatifs;
- une **justification claire** de stratégies d'atténuation des risques et de mesures de protection rentables pour répondre aux exigences opérationnelles; et
- une **piste de vérification transparente** et un **compte rendu des décisions en matière de gestion des risques** pour prouver la diligence raisonnable et la responsabilisation et, ainsi, satisfaire aux obligations réglementaires et aux exigences de la politique.

La méthodologie harmonisée d'évaluation des menaces et des risques est conçue pour tous les employés, les biens et les services menacés. De plus, elle peut facilement être intégrée aux méthodologies de gestion de projet et aux cycles de développement de système. L'analyse peut être effectuée à n'importe quel niveau de granularité, des vastes profils de risque ministériels aux examens très ciblés de problèmes particuliers, pour répondre aux besoins de la direction pour des solutions adaptées aux niveaux à la fois stratégiques et opérationnels. L'utilisation d'outils communs peut promouvoir l'interopérabilité lorsque l'on doit gérer des risques à l'échelle d'installations partagées et de systèmes interconnectés de technologie de l'information, aspects de plus en plus importants lorsque les responsabilités relatives à la prestation de service transcendent les frontières organisationnelles. Enfin, dans l'esprit de la fonction moderne de contrôleur, des paramètres objectifs et des rapports analytiques appuient le cadre de responsabilisation de gestion pour l'évaluation des résultats et du rendement, en particulier pour ce qui touche la gestion des risques, la gérance et la responsabilisation. Les interrelations de ces éléments importants de la fonction moderne de contrôleur sont illustrées dans la figure AG-3.

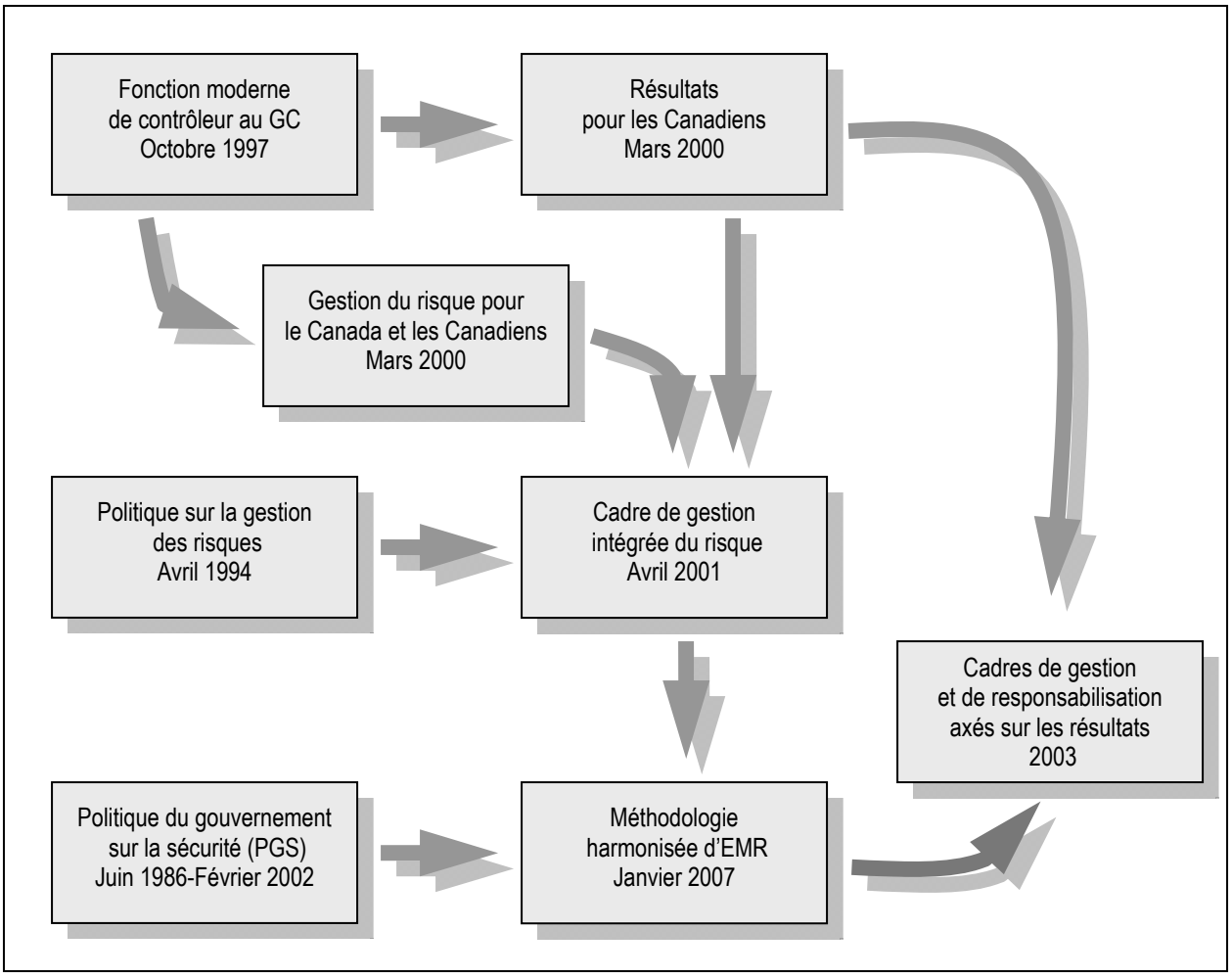

Figure AG-3: Méthodologie harmonisée d'EMR à l'appui de la fonction moderne de contrôleur

Sommaire de gestion

1 Introduction

> « On doit sauvegarder les biens selon des exigences sécuritaires de base et une gestion continue des risques pour la sécurité. »
>
> *Politique du gouvernement sur la sécurité*, février 2002

Au niveau le plus élevé, la *Politique du gouvernement sur la sécurité* (PGS) prescrit deux approches complémentaires de la gestion des risques pour la sécurité.

La première est l'application des exigences de base en matière de sécurité, ou normes de sécurité minimales, précisées dans la politique elle-même ou dans des documents à l'appui, plus précisément les normes opérationnelles de sécurité et la documentation technique décrites à la section 9 de la PGS. Les exigences de base en matière de sécurité offrent de nombreux avantages, dont la facilité d'utilisation, une uniformité accrue et, par conséquent, une plus grande interopérabilité, pour n'en nommer que quelques-uns. Cependant, compte tenu du temps qu'il faut pour élaborer des normes efficaces, l'évolution rapide des technologies fait que bon nombre d'entre elles sont périmées. En outre, le choix des contre-mesures peut être limité et, comme il s'agit de normes minimales, elles pourraient ne pas être suffisantes pour les biens de plus grande valeur exposés à des menaces plus graves.

Pour répondre à ces préoccupations, la PGS prévoit un complément efficace, soit une gestion continue des risques sous la forme de l'évaluation des menaces et des risques (EMR).

Bien que les exigences de base en matière de sécurité et les EMR soient très différentes, ces deux approches de la gestion des risques sont totalement complémentaires[1]. Ainsi, un gestionnaire peut effectuer une EMR informelle ou une vérification superficielle de l'environnement de risque pour déterminer si les exigences de base en matière de sécurité sont pertinentes. Il peut ensuite, au besoin, effectuer une EMR exhaustive pour corriger toute lacune.

Si une évaluation exhaustive est nécessaire, la section 10.7 de la politique, Gestion des risques pour la sécurité, décrit un processus d'EMR en quatre étapes :

- déterminer **la portée de l'évaluation** et **identifier les employés et les biens** à sauvegarder;
- identifier les **menaces envers les employés et les biens** au Canada et à l'étranger, et évaluer la probabilité qu'elles se concrétisent et leur incidence;
- évaluer les **risques** en fonction de la pertinence des **mesures de sauvegarde existantes et des vulnérabilités**;

[1] L'appendice A-2 examine plus longuement la relation entre les normes de sécurité, les EMR, tant officielles qu'informelles, et d'autres démarches de gestion des risques.

- mettre en œuvre toute **mesure supplémentaire** qui réduira les risques à un niveau acceptable.

D'autres exigences de la politique développent certaines étapes du processus et indiquent dans quels cas des EMR doivent être effectuées afin d'obtenir des solutions de sécurité rentables pour assurer la protection des employés et des biens ainsi que la prestation des services. Bien que les normes opérationnelles de sécurité portant sur l'identification des biens, la gestion des risques pour la sécurité, la sécurité matérielle, la gestion de la sécurité des TI et la planification de la continuité des activités exposent dans le détail ces exigences de la politique, des explications plus détaillées encore sont nécessaires pour mener à bien concrètement un projet officiel d'EMR et obtenir des résultats probants. C'est la raison pour laquelle la *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)* a été élaborée, en tant qu'outil pratique fournissant des précisions sur la politique et les normes à l'appui, comme on peut le voir dans la figure SG-1, afin d'aider les gestionnaires du gouvernement à atteindre les objectifs et à respecter les exigences de la PGS.

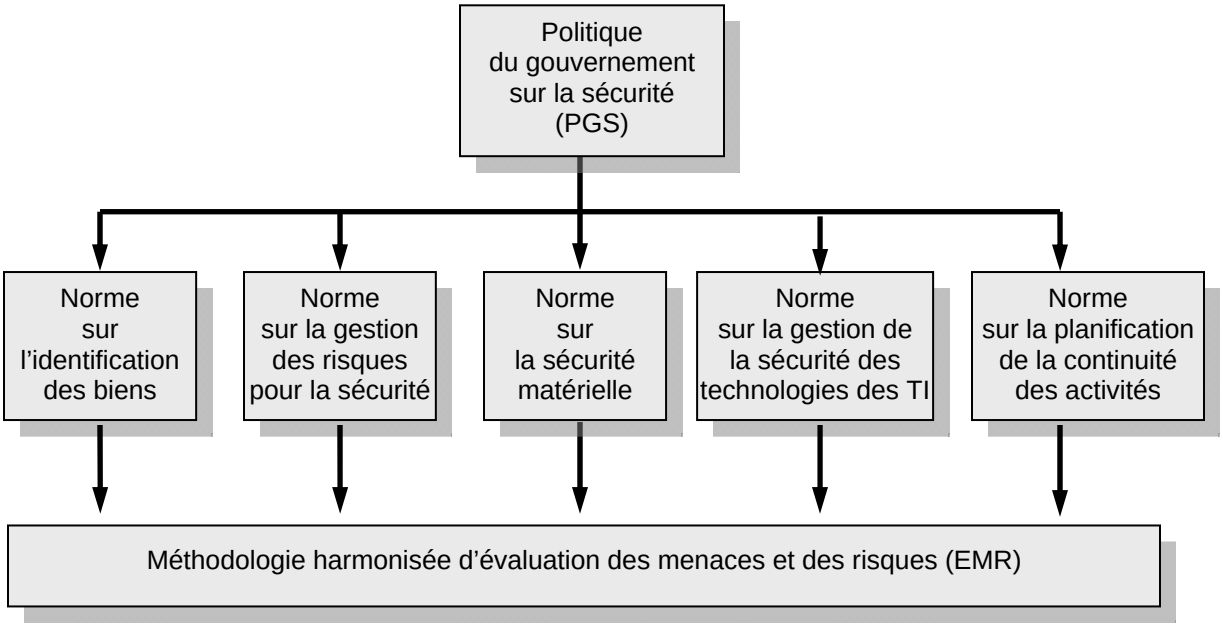

Figure SG-1 : Cadre contextuel de la méthodologie harmonisée d'EMR

La méthodologie harmonisée d'EMR présente l'EMR comme un projet réalisé en cinq phases distinctes, comprenant chacune au moins trois processus, comme on peut le voir dans la figure SG-2. La première phase vise à établir le mandat et la portée du projet. Les trois suivantes ont pour but de déterminer l'environnement de risque en examinant les biens et leur valeur, ainsi que les menaces et les vulnérabilités inclus dans la portée de l'évaluation. La dernière phase est celle où l'équipe fait ses recommandations sur l'acceptabilité des risques résiduels et, au besoin, formule les stratégies d'atténuation et les mesures de protection. L'EMR n'est donc qu'un simple projet officiel de collecte et d'analyse des données pertinentes dans le but de déterminer les niveaux de risques et de recommander des mesures de protection efficientes et rentables au besoin.

Les phases de l'EMR et les processus connexes sont expliqués brièvement dans le reste du présent résumé et développés considérablement dans les annexes et appendices qui suivront.

2 Préparation

2.1 Généralités

Une planification soignée et une réflexion préalable sont essentielles à l'obtention de résultats utiles dans un projet d'EMR.

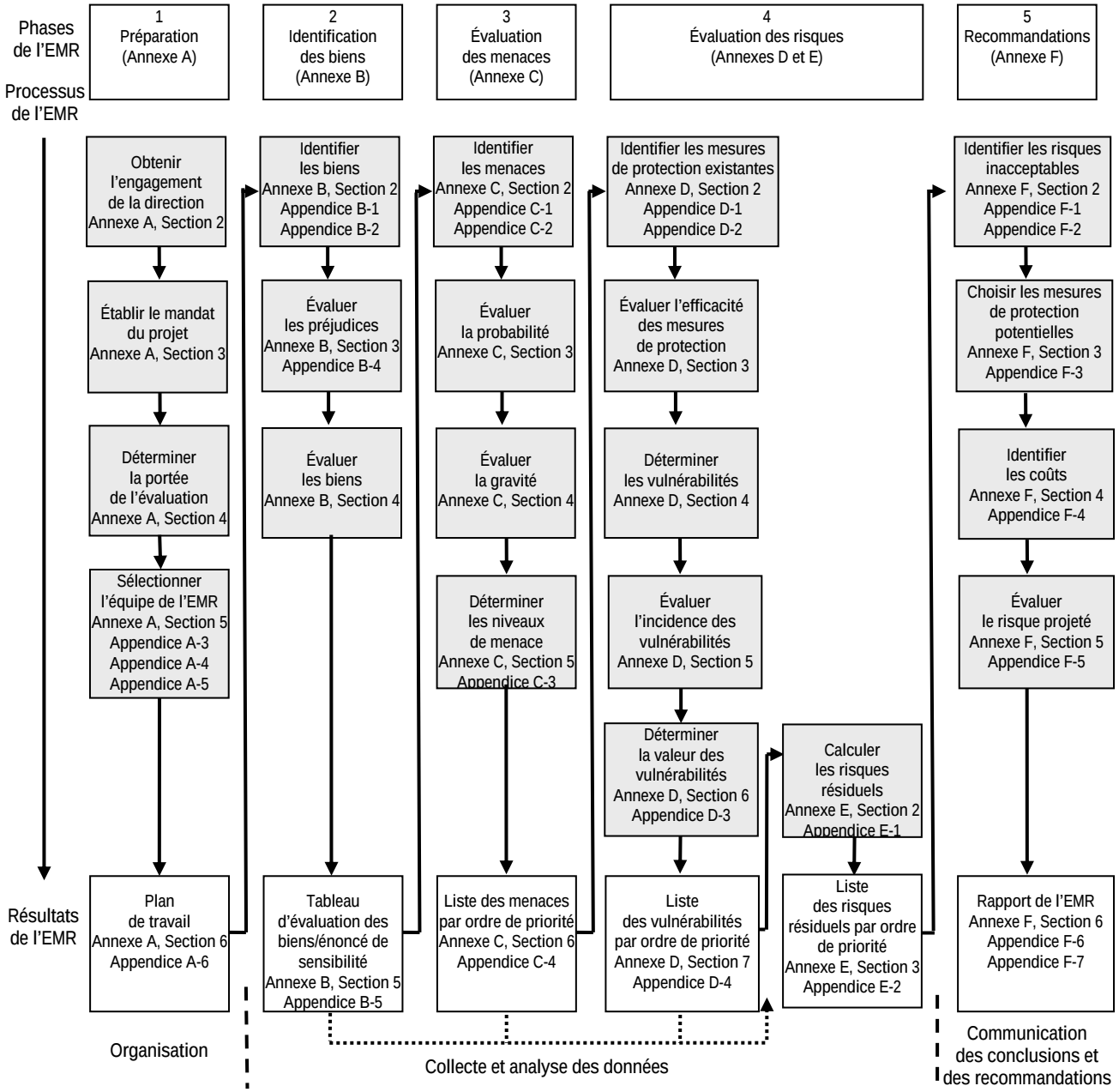

Figure SG-2 : Phases et processus d'un projet d'EMR

2.2 Engagement de la direction

Pour pouvoir prendre des décisions éclairées sur l'acceptabilité de tout risque résiduel, les cadres supérieurs du ministère doivent bien comprendre les EMR et leur rôle dans un programme global de gestion des risques. L'engagement et le soutien de la direction sont également nécessaires pour établir un mandat clair, mobiliser les ressources nécessaires et faciliter la collecte des données indispensables à une évaluation équilibrée.

2.3 Mandat d'un projet d'EMR

Les cadres supérieurs confèrent habituellement la responsabilité de la réalisation d'une EMR à un seul bureau ou représentant possédant une connaissance suffisante à la fois des opérations et de la méthodologie d'EMR choisie. Le représentant désigné doit d'abord clarifier l'objet du projet d'EMR afin de confirmer à la fois la faisabilité de l'exercice et la nécessité d'une évaluation. Une fois ces éléments examinés et acceptés, les rôles et responsabilités relatifs doivent être précisés, particulièrement pour le responsable de l'acceptation des risques. Parmi les autres questions à examiner figurent la priorité du projet, les attentes de la direction et la présentation de rapports, qui doivent toutes être consignées dans le plan de travail du projet d'EMR, tel qu'il est indiqué à la section 2.7 ci-après.

2.4 Portée d'un projet d'EMR

De nombreuses EMR échouent parce que la portée de l'évaluation n'est pas clairement définie au début du projet. Comme cela entraîne presque inévitablement un gaspillage d'efforts et des retards inutiles, il est important de déterminer l'objet de l'évaluation, le niveau de détail nécessaire et les limites de l'exercice dès le départ. En règle générale, les EMR les plus efficaces sont aussi courtes que possible compte tenu de la nécessité d'une prise de décisions éclairée. Pour atteindre cet idéal avec de plus gros projets ou des biens plus complexes, il est souvent préférable de réaliser plusieurs évaluations modulaires plus petites qu'un seul projet massif. Évidemment, il est possible de réviser la portée d'un projet à tout moment si les circonstances changent, par exemple si l'on découvre des menaces ou des vulnérabilités inconnues jusque-là. Compte tenu de tout cela, voici quelques-uns des facteurs à prendre en considération au moment de déterminer la portée d'une EMR :

- le **stade dans le plan du projet** ou le **cycle de développement des systèmes** − davantage de précisions seront nécessaires à mesure que les projets évoluent, de la définition des exigences initiales à la conception détaillée, au développement et enfin à la mise en œuvre finale;
- l'**environnement de risque** – parce qu'une analyse plus exhaustive, plus approfondie s'impose généralement pour les employés, les biens et les services exposés à un plus grand risque, une évaluation superficielle peut être nécessaire au départ pour caractériser l'environnement de risque;
- l'**objet du projet d'EMR** – les évaluations ministérielles se situent habituellement à un haut niveau et reposent sur de larges bases, alors que celles des grands projets de l'État

sont souvent très détaillées; inversement, des EMR très courtes et ciblées sont idéales pour répondre à des préoccupations particulières en matière de sécurité;
- les **contraintes de temps et d'argent** – inévitablement, des considérations pratiques peuvent limiter la portée pour des raisons légitimes, mais même une EMR à un niveau plus élevé peut répondre aux besoins de la direction.

2.5 Composition de l'équipe

Les EMR plus petites peuvent être réalisées par une seule personne, mais la plupart nécessitent un effort d'équipe pour rassembler les renseignements et l'expertise nécessaires à une évaluation efficace. En général, les équipes chargées de projets plus gros et plus complexes doivent compter plus de membres, mais même les projets plus simples et plus ciblés nécessiteront un accès à des employés ayant différentes connaissances et habiletés. Afin de veiller à ce que l'évaluation repose sur des renseignements pertinents, les responsables suivants y participent directement à titre de membres de l'équipe ou à tout le moins y contribuent :

- les **gestionnaires de programmes ou gestionnaires opérationnels** comprennent l'importance opérationnelle des employés, des biens et des services qu'ils offrent, ainsi que le préjudice qui pourrait résulter d'une compromission, de sorte que leur contribution est essentielle à la phase d'identification et d'évaluation des biens de l'évaluation;
- les **gestionnaires de projet** et leurs employés traduisent les exigences fonctionnelles ou opérationnelles en solutions techniques, de sorte qu'ils peuvent apporter une contribution importante au processus d'identification des biens et à l'évaluation subséquente des vulnérabilités;
- les **gestionnaires des installations**, les **dirigeants principaux de l'information** et leurs employés peuvent fournir des renseignements précieux sur les locaux partagés et les infrastructures techniques dans le cadre du processus d'identification des biens et de l'évaluation des vulnérabilités;
- les **responsables ministériels de la sécurité**, à savoir l'agent de sécurité du ministère (ASM), le coordonnateur de la sécurité des TI (CSTI) et le coordonnateur de la planification de la continuité des activités (CPCA), peuvent fournir aide et conseils sur le contexte de la menace et les mesures de protection possibles.

2.6 Autres ressources

Selon la portée et l'objet d'un projet d'EMR, d'autres ressources ministérielles, des coordonnateurs de la protection des renseignements personnels aux employés de la santé et de la sécurité au travail en passant par les gestionnaires des services financiers et des services du matériel, sans oublier les vérificateurs internes et les conseillers juridiques, peuvent fournir des détails utiles pour compléter les données recueillies par les principaux membres de l'équipe. Les ressources externes auxquelles l'équipe de l'EMR a accès peuvent comprendre les ministères responsables en matière de sécurité, définis à l'appendice A de la PGS, et divers consultants du secteur privé possédant des qualifications techniques ou professionnelles pertinentes.

2.7 Plan de travail de l'EMR

Afin d'assurer un effort coordonné qui réponde aux besoins opérationnels des gestionnaires des programmes et des cadres supérieurs ministériels, l'équipe de l'EMR doit élaborer un plan de travail exhaustif, cette étape étant sa première tâche importante. Ce plan doit être approuvé par le responsable de l'acceptation des risques qui, en dernier ressort, examinera les recommandations et acceptera ou rejettera les risques résiduels prévus recensés dans le rapport d'EMR. Le niveau de détail exact variera en fonction de la portée et de l'ampleur de l'évaluation, mais le plan doit au moins décrire les éléments suivants :

- le mandat établi, l'objet, la portée et les modalités de l'EMR;
- les principaux membres de l'équipe et les autres ressources à leur disposition, avec de brefs mandats pour chacun;
- les contributions applicables au projet, comme les documents liés aux EMR antérieures, les évaluations des facteurs relatifs à la vie privée (EFVP), les analyses des répercussions sur les opérations (ARO), les documents de conception, les plans d'étage des installations, les inventaires et tout protocole d'entente (PE) pertinent concernant le partage des renseignements ou d'autres biens;
- un calendrier avec les dates fixées pour chaque produit livrable de la phase de l'identification des biens aux recommandations finales dans le rapport de l'EMR;
- les dispositions logistiques pertinentes, comme les besoins en filtrage de sécurité, en soutien administratif et en ressources, ce qui comprend la source des fonds pour chacune des dépenses connexes, comme les marchés avec les consultants.

3 Identification et évaluation des biens

Une fois la phase de préparation terminée, l'équipe de l'EMR peut commencer à identifier et à évaluer les biens. Cette phase d'un projet d'EMR comprend concrètement trois processus différents, mais étroitement liés. Premièrement, tous les employés, les biens et les services inclus dans la portée de l'évaluation doivent être identifiés suffisamment en détail pour qu'il soit possible de déterminer lesquels pourraient avoir besoin de protection. Ensuite, il faut évaluer le degré de préjudice qui pourrait vraisemblablement résulter d'une atteinte à leur confidentialité, à leur disponibilité ou à leur intégrité conformément à la *Norme opérationnelle de sécurité sur l'identification des biens*. Puis, en se fondant sur cette évaluation, il faut attribuer des valeurs relatives pour catégoriser les biens et les services, plus particulièrement. Tous les biens ont une ou plusieurs valeurs liées à leur confidentialité, leur disponibilité ou leur intégrité.

Pour faciliter l'identification des biens à un niveau approprié de détail, la méthodologie harmonisée d'EMR propose une liste hiérarchique exhaustive des biens. Afin de favoriser une évaluation cohérente des biens et de permettre l'analyse comparative de biens différents ou de valeurs différentes pour le même bien, le guide contient aussi un tableau des préjudices dont les valeurs vont de très faible à très élevé.

Le résultat final de la phase d'identification et d'évaluation des biens d'un projet d'EMR, aussi appelé énoncé de sensibilité, est une simple liste des employés, des biens et des services avec les

valeurs relatives qui leur ont été attribuées en fonction des préjudices ou de l'incidence sur les opérations qui pourraient résulter d'une compromission.

4 Évaluation des menaces

Une fois la phase d'identification et d'évaluation des biens terminée, l'équipe de l'EMR doit identifier toute menace qui pourrait vraisemblablement causer un préjudice aux employés, aux biens ou à la prestation des services identifiés pendant la deuxième phase. Toutes les menaces, qu'elles soient d'origine humaine (délibérées ou accidentelles) ou le résultat de risques naturels, sont considérées à un niveau de détail proportionnel à la portée de l'évaluation. Pour qu'il soit possible de faire la distinction entre les diverses menaces et de déterminer lesquelles sont les plus susceptibles de susciter de graves préoccupations, chaque menace est évaluée en fonction de la **probabilité** qu'elle se concrétise et de la **gravité** de son incidence.

Étant donné les incertitudes qui entourent la majorité des menaces, les analystes se heurtent souvent à de sérieuses difficultés dans cette phase d'un projet d'EMR. C'est pourquoi, pour faciliter l'identification des menaces à un niveau approprié de détail, la méthodologie harmonisée d'EMR propose une liste hiérarchique exhaustive des menaces. Puis, afin de favoriser une analyse comparative des différentes menaces, le guide contient aussi des paramètres simples pour la probabilité et la gravité des menaces éventuelles, ce qui permet d'arriver à des valeurs des menaces allant de très faible à très élevée.

Le résultat final de la phase d'évaluation des menaces d'un projet d'EMR est une simple liste des menaces avec des valeurs relatives témoignant de la probabilité qu'elles se concrétisent et de la gravité de leur incidence éventuelle sur la confidentialité, la disponibilité et l'intégrité.

5 Évaluation des risques

5.1 Généralités

La quatrième phase d'un projet d'EMR, l'évaluation des risques, est subdivisée en deux étapes séquentielles. La première comprend cinq processus visant à évaluer les vulnérabilités qui ont une incidence sur les employés, les biens et les services identifiés pendant la deuxième phase, qui pourraient être exploitées par les menaces cataloguées pendant la troisième phase. La deuxième étape de l'évaluation des risques prévoit un seul processus de calcul des risques résiduels résultant de chaque combinaison de biens avec les menaces et les vulnérabilités connexes.

5.2 Évaluation des vulnérabilités

Pour évaluer les vulnérabilités, l'équipe de l'EMR doit mesurer l'efficacité des mesures de protection existantes et de celles dont la mise en œuvre est en cours. L'analyse de ces données fera ressortir toutes les caractéristiques des employés et des biens ou du contexte dans lequel ils se trouvent qui les rendent susceptibles à une compromission. L'évaluation des vulnérabilités peut être compliquée par une perception erronée courante qu'il s'agit toujours de faiblesses ou de

défauts. De nombreuses vulnérabilités sont effectivement des caractéristiques négatives, mais d'autres sont des qualités positives qui pourraient simplement avoir des effets secondaires indésirables. Par exemple, la portabilité des ordinateurs portatifs est un avantage souhaitable pour lequel on paie un prix plus élevé, mais un avantage qui les rend plus susceptibles au vol. C'est pourquoi, pour faciliter la réalisation d'une évaluation équilibrée des vulnérabilités, la méthodologie harmonisée d'EMR propose une longue liste de vulnérabilités contenant des renvois judicieux à la liste des mesures de protection présentée dans la phase des recommandations. Comme pour les valeurs des biens et des menaces, des paramètres simples sont établis pour coter les différentes vulnérabilités de très faible à très élevée.

5.3 Calcul des risques résiduels

Après avoir identifié les biens (ce qui comprend les employés et les services), les menaces et les vulnérabilités et y avoir attribué des valeurs, il ne reste plus qu'à calculer le produit des trois variables pour établir une liste par ordre de priorité des risques résiduels évalués aux fins d'analyse durant la phase des recommandations d'un projet d'EMR.

6 Recommandations

Après avoir identifié les risques résiduels évalués, leur avoir attribué des niveaux relatifs de Très faible à Très élevé et les avoir classés par ordre de priorité, l'équipe de l'EMR doit préparer des recommandations adéquates pour le responsable de l'acceptation des risques.

Si les risques résiduels évalués sont totalement acceptables pour l'équipe de direction (généralement ceux cotés Très faible et Faible et peut-être certains cotés Moyen), il devrait suffire de recommander le maintien des mesures de protection existantes et l'achèvement de celles dont la mise en œuvre est en cours, ainsi qu'une surveillance constante de leur efficacité.

Dans certains cas, si les risques résiduels évalués sont cotés Très faible, il peut être faisable de recommander la suppression de certains mécanismes de protection et l'acceptation de risques de niveau légèrement plus élevé pour réaliser des économies souhaitables ou améliorer l'efficience opérationnelle.

Dans les cas où les risques résiduels évalués sont inacceptables (généralement ceux cotés Très élevé et Élevé et peut-être certains cotés Moyen), certaines mesures correctives s'imposent généralement. Pour faciliter le choix d'une réponse adéquate, la méthodologie harmonisée d'EMR comprend une longue liste de mesures de protection contenant des renvois aux vulnérabilités qu'elles corrigent, aux menaces qu'elles atténuent et aux biens (ou aux employés et aux services) qu'elles protègent. De plus, des critères explicites de sélection des mesures de protection sont expliqués en détail pour faciliter l'analyse comparative de leur efficacité et de leur coût relatif. Enfin, les risques résiduels évalués découlant de l'évaluation des risques sont révisés pour tenir compte des améliorations escomptées une fois les recommandations totalement appliquées. Dans le rapport final d'EMR, ces risques sont présentés sous la forme de risques résiduels prévus.

7 Conclusion

7.1 Généralités

La méthodologie harmonisée d'EMR décrit l'EMR comme un projet réalisé en cinq phases distinctes, comprenant chacune au moins trois processus. Les relations relatives entre ces phases et processus sont illustrées dans la figure SG-2.

Il est possible d'entreprendre en parallèle certains processus de l'EMR afin d'améliorer le calendrier et d'optimiser l'utilisation de ressources limitées. Ainsi, si des déplacements sont nécessaires pour recueillir des données sur les biens, les employés, les services et leurs valeurs, il est très logique de recueillir les données sur les menaces locales en même temps pour éviter un autre déplacement. Dans la plupart des cas, cependant, les phases et processus de l'EMR doivent être complétés séquentiellement parce que le résultat d'une phase est généralement nécessaire pour déterminer l'effort déployé pendant la prochaine. Ainsi, il peut être faisable de commencer la phase d'évaluation des menaces avant que l'identification des biens soit terminée, mais les menaces les plus préoccupantes ne seront pas totalement évidentes tant que les biens qui ont le plus de valeur n'auront pas été identifiés. De même, il est possible que certaines vulnérabilités génériques soient évidentes dès le départ, mais d'autres n'apparaîtront qu'une fois que les biens auront été bien compris. Même l'évaluation des menaces déterminera l'évaluation des vulnérabilités dans la mesure où on consacre normalement plus d'attention aux vulnérabilités les plus susceptibles d'être exploitées par les menaces les plus sérieuses. Les divers processus à l'intérieur d'un projet d'EMR sont donc généralement entrepris successivement, comme l'illustre la figure SG-2.

7.2 Projets d'EMR et gestion des risques

Le résultat d'un projet d'EMR, le rapport d'EMR, est un document statique, évaluant les variables des risques à un moment précis pour un ensemble donné de biens dans une configuration donnée. Par contre, les exigences opérationnelles ne sont pas statiques, ni les programmes, les services et les biens qui y sont associés et qui changent avec le temps, tout comme les menaces qui peuvent avoir une incidence sur eux. De nouvelles vulnérabilités sont aussi découvertes régulièrement, surtout dans le secteur complexe des technologies de l'information. C'est pourquoi, dans un contexte essentiellement dynamique comme celui-là, une gestion continue des risques est essentielle.

Pour satisfaire à cette exigence fondamentale, les gestionnaires doivent d'abord surveiller la mise en œuvre des recommandations approuvées de l'EMR. Puis, à mesure que les circonstances changent, l'évaluation doit être revue et mise à jour lorsque les variables de risques, plus précisément les valeurs des biens, les menaces ou les vulnérabilités, évoluent considérablement. Le fait d'avoir une méthodologie d'EMR officielle simplifie les choses considérablement, cependant, parce qu'il n'est pas nécessaire de refaire toute l'évaluation, seulement les portions touchées par les changements.

Les relations entre un projet d'EMR et la gestion continue des risques avec les points décisionnels connexes sont illustrées dans la figure SG-3.

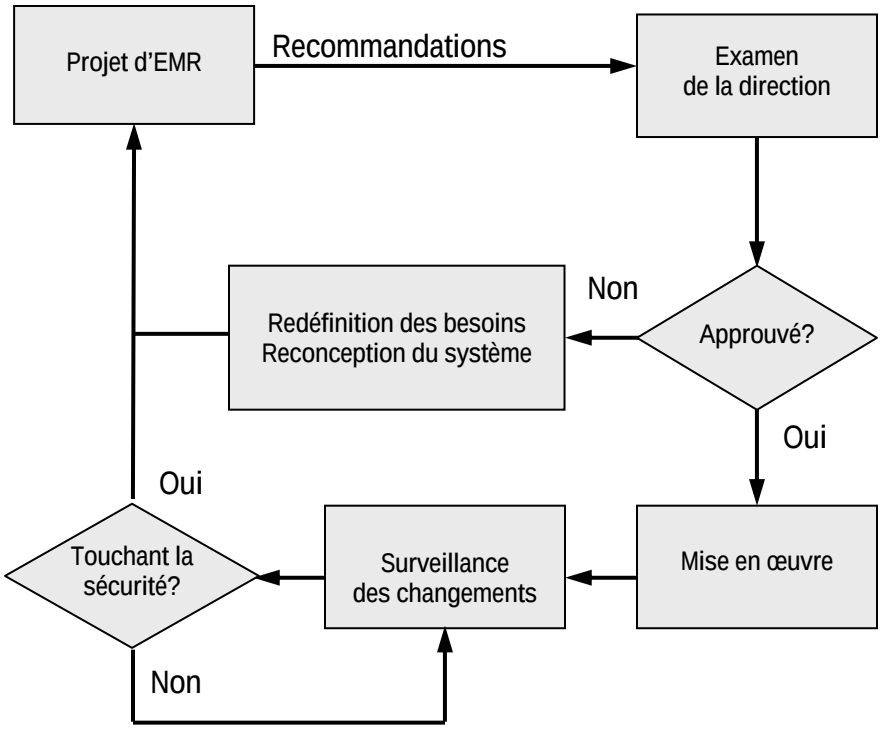

Figure SG-3 : Modèle (très) simplifié de gestion des risques

Annexe A - Phase de préparation

1 Introduction

1.1 Généralités

Presque inévitablement, un projet d'EMR prendra beaucoup plus de temps et coûtera considérablement plus cher que nécessaire s'il est réalisé sans une planification et une préparation adéquates. Des contributions importantes peuvent être oubliées, entraînant des hypothèses inexactes et une analyse déficiente. Des mesures de protection essentielles peuvent être omises, laissant des employés ou des biens et les services connexes exposés à des risques, alors que d'autres qui ne conviennent pas peuvent être retenues, imposant de ce fait des coûts et des restrictions inutiles aux opérations.

La phase de préparation d'un projet d'EMR vise à éviter ces pièges éventuels et compte quatre processus importants débouchant sur un résultat concret :

- **Engagement de la direction** – s'assurer que la haute direction comprend le rôle de l'EMR dans le soutien du Cadre de gestion intégrée du risque et ses propres responsabilités dans l'établissement et l'approbation de niveaux acceptables de risques résiduels.
- **Mandat du projet d'EMR** – clarifier les rôles et les responsabilités et identifier explicitement le responsable de l'acceptation des risques.
- **Portée de l'évaluation** – fixer des limites raisonnables à l'EMR en fonction de l'objet de l'évaluation et de l'environnement de risque.
- **Composition de l'équipe** – réunir les bons employés, qui ont les connaissances et les habiletés nécessaires pour recueillir les renseignements essentiels, analyser les données et recommander des solutions valables pour atteindre les objectifs opérationnels de l'organisation.
- **Plan de travail de l'EMR** – déterminer les ressources nécessaires, répartir les responsabilités équitablement et établir un calendrier réaliste pour les activités de l'EMR.

1.2 But

Le but de cette annexe est de décrire les quatre processus et le résultat unique de la phase de préparation d'un projet d'EMR.

2 Engagement de la direction

2.1 Généralités

L'application réussie d'une méthodologie d'EMR à l'intérieur d'un programme de sécurité ministériel et du Cadre de gestion intégrée du risque dépend de la compréhension et du soutien de la haute direction pour deux raisons surtout. Premièrement, une large compréhension de l'EMR et de son rôle à l'intérieur d'un programme exhaustif de gestion des risques est essentielle à la prise de décisions éclairées sur la stratégie d'atténuation des risques et les mesures de protection nécessaires pour atteindre les objectifs opérationnels. Deuxièmement, d'un point de vue plus pratique encore, il pourrait être difficile d'obtenir les ressources nécessaires pour réaliser une EMR et la collaboration de toutes les parties associées à l'évaluation sans l'engagement de la haute direction à l'égard du processus.

2.2 Compréhension de la direction

Au gouvernement, les gestionnaires sont responsables de la sécurité des employés et des biens ainsi que de la prestation continue des services. Dans certains cas, le poids de ces responsabilités engendre une culture d'aversion pour le risque, une réticence à accepter le moindre risque susceptible de compromettre des employés, des biens ou des services. Malheureusement, cette attitude peut faire rater des occasions d'améliorer les services. Dans d'autres cas, pour profiter des avantages de nouvelles technologies, certains gestionnaires deviennent très tolérants aux risques, mettant de ce fait en danger des employés, des biens ou des services. Pour parvenir à un équilibre efficace entre ces deux extrêmes, c.-à-d. pour éviter une aversion excessive pour le risque et une tolérance injustifiée aux risques, il faut comprendre et accepter la gestion des risques. Plus précisément, les cadres supérieurs et les gestionnaires de programmes doivent être conscients des éléments suivants :

- la nature et l'importance du risque résiduel avant de l'accepter;
- le rôle de la méthodologie d'EMR en tant qu'outil à l'appui des décisions de gestion des risques;
- la nécessité d'une analyse objective pour parvenir à des solutions opérationnelles rentables;
- la valeur d'une piste de vérification transparente pour documenter la diligence raisonnable si des risques devaient se concrétiser et des préjudices en résulter.

2.3 Ressources et collaboration

La méthodologie harmonisée d'EMR s'emploie à simplifier considérablement les processus des EMR officielles, mais l'effort peut encore être substantiel, surtout pour des installations et des systèmes plus gros ou plus complexes. Il est donc essentiel de pouvoir compter sur des ressources humaines et financières adéquates afin de pouvoir réaliser une évaluation dans les délais impartis pour atteindre les objectifs opérationnels. Il est également nécessaire d'avoir accès à des employés expérimentés ainsi qu'à l'installation ou au système examiné pour recueillir les données qui devront ensuite être analysées. Si les cadres supérieurs comprennent le

processus d'EMR et y croient en tant qu'outil efficace à l'appui d'une saine gestion des risques, ces questions et d'autres problèmes éventuels sont moins susceptibles de nuire à un projet d'EMR. Bref, des gestionnaires compréhensifs peuvent :

- **Approuver/allouer des ressources.** Évidemment, les besoins en ressources pour réaliser un projet d'EMR varieront en fonction de la portée et de la complexité de l'effort. Néanmoins, les cadres supérieurs sont plus susceptibles d'approuver les ressources humaines et financières nécessaires à une évaluation s'ils comprennent le processus et ses avantages. Cela est particulièrement important dans le contexte d'un projet assujetti à de graves contraintes financières, où l'EMR peut être vu comme un détournement de ressources essentielles à d'autres activités importantes.
- **Assurer un effort d'équipe.** Une saine tension entre les responsables des projets et des programmes peut avoir des avantages positifs dans la recherche de solutions équilibrées et rentables. Une relation semblable entre les conseillers en matière de sécurité et les employés des programmes ou des projets peut être tout aussi bénéfique. Malheureusement, les différents points de vue de chaque groupe peuvent, dans certains cas, provoquer de graves frictions et un gaspillage d'énergie qui va à l'encontre du but recherché. Si la direction s'est engagée à élaborer des solutions rentables fondées sur une saine gestion des risques, la plupart des différends peuvent être réglés afin d'assurer un effort d'équipe concerté en vue de l'atteinte d'objectifs communs.
- **Autoriser l'accès aux installations ou aux systèmes.** Les entrevues et les inspections sur place sont souvent de précieuses sources de renseignements en vue d'une évaluation. Dans certains cas, cependant, elles peuvent être considérées comme intempestives ou perturbant les opérations quotidiennes. Il est beaucoup plus facile de surmonter ces réserves si les autorités responsables connaissent la valeur du processus d'EMR en tant qu'outil d'analyse à l'appui de décisions efficaces en matière de gestion des risques.
- **Promouvoir le partage de l'information.** Trop souvent, les employés et les gestionnaires sont réticents à faire abstraction des structures organisationnelles pour partager de l'information, surtout sur des sujets aussi sensibles que les menaces et les vulnérabilités. Comme ces données sont essentielles à une évaluation éclairée, le soutien de la gestion est inestimable pour aider à faire tomber les obstacles à une communication et un partage de l'information efficaces.

2.4 Considérations pratiques

Si les cadres supérieurs comprennent que le Cadre de gestion intégrée du risque est l'un des piliers de la fonction moderne de contrôleur, beaucoup d'entre eux connaissent moins bien le processus d'EMR en tant qu'outil à l'appui d'une saine prise de décisions. Par conséquent, pour bénéficier des avantages susmentionnés, il pourrait être bon d'examiner plus attentivement quelques mesures pratiques visant à les sensibiliser davantage à l'EMR et à les aider à l'accepter :

- offrir des **séances d'information pour cadres supérieurs** afin d'expliquer la méthodologie harmonisée d'évaluation des menaces et des risques, ses relations avec le

Cadre de gestion intégrée du risque et les avantages escomptés d'une analyse objective pour parvenir à des solutions rentables[1];

- harmoniser la méthodologie d'EMR avec les **processus de planification stratégique** afin d'assurer une utilisation constante au niveau le plus élevé;
- intégrer la méthodologie d'EMR à **d'autres processus de gestion**, comme le cycle de planification opérationnelle ou le cycle de développement des systèmes, afin qu'elle devienne une autre activité régulière;
- **définir clairement les pouvoirs** dans les politiques ministérielles sur la réalisation des EMR et le règlement de tout différend entre les employés des programmes, des projets ou de la sécurité.

3 Mandat du projet d'EMR

Avant de commencer un projet officiel d'EMR, il est particulièrement important de définir clairement le mandat de l'évaluation. À cette fin, le cadre supérieur responsable des installations, des services ou des systèmes de TI à l'étude désigne normalement un chef d'équipe d'EMR compétent en se fondant sur plusieurs facteurs examinés dans les sections 5.3 et 5.4.7 ci-après. Cette personne doit recevoir des instructions explicites :

- lui attribuant les pouvoirs nécessaires pour réaliser le projet d'EMR;
- lui expliquant les attentes de la direction en ce qui a trait aux risques résiduels et aux priorités opérationnelles;
- définissant les rôles, les responsabilités, les liens hiérarchiques et les pouvoirs d'approbation pour le plan de travail de l'EMR et pour les résultats de chacune des phases subséquentes du projet, particulièrement le responsable de l'acceptation des risques recensés dans le rapport d'EMR final.

Par la suite, ces instructions doivent être incorporées dans le plan de travail de l'EMR.

4 Portée de l'évaluation

4.1 Généralités

Avant de commencer un projet d'EMR, il est particulièrement important de déterminer la portée de l'évaluation, de décider quels employés, biens et services seront examinés et à quel niveau de détail. Si on ne fixe pas des limites réalistes dès le départ, les étapes subséquentes de collecte et d'analyse des données risquent de ne plus finir et le projet, de s'enliser sous le poids de l'effort. À l'autre extrême, il est possible d'effectuer une évaluation à un niveau tellement élevé que des questions importantes demeurent sans réponse et que les risques résiduels ne sont pas totalement

[1] L'**aperçu général** situe le processus d'EMR à l'intérieur de la fonction moderne de contrôleur à l'intention des publics de plus haut niveau. Comme il est indiqué dans l'introduction, le CST et la GRC ont aussi élaboré un programme de sensibilisation à l'intention des cadres supérieurs et des membres de la haute direction.

compris. Pour éviter ces problèmes, il faut que la première étape du processus de planification initiale soit de déterminer clairement l'étendue et la profondeur de l'évaluation.

4.2 Facteurs de planification

4.2.1 Vue d'ensemble

Pour assurer la cohérence des rapports d'EMR, il faut tenir compte de plusieurs facteurs à l'étape de la définition de la portée, dont l'objet de l'évaluation, le stade où en est le plan d'un projet ou le cycle de développement d'un système, l'environnement de risque et les préoccupations pratiques relatives aux contraintes de temps ou d'argent.

4.2.2 Objet de l'évaluation

Les rapports d'EMR ont de nombreux usages différents qui vont des évaluations de haut niveau reposant sur de larges bases aux examens très ciblés de préoccupations particulières en matière de sécurité. Dans chaque cas, la portée de l'évaluation doit être ajustée en fonction de l'objectif convenu et, comme il est indiqué dans la section 6, l'objectif de l'évaluation doit être énoncé clairement dans le plan de travail de l'EMR. Voici quelques-unes des plus importantes raisons de réaliser une EMR :

- **Évaluations ministérielles.** Étant donné la taille et la complexité de nombreuses institutions gouvernementales, les évaluations ministérielles sont généralement réalisées à un niveau de détail très élevé où la portée est, inévitablement, très étendue mais relativement peu profonde, l'objectif étant de se concentrer sur les risques stratégiques liés aux principaux secteurs opérationnels et aux groupes de biens connexes. Bien qu'elles ne soient pas aussi détaillées que les rapports d'EMR plus ciblés axés sur une seule installation, un seul réseau ou un seul service, les évaluations ministérielles sont très utiles pour bien asseoir le programme global de sécurité, classer les divers projets d'EMR par ordre de priorité et établir un cadre contextuel général pour leur examen.
- **Grands projets de l'État (GPE).** Par définition, les GPE sont ceux dont le coût total prévu dépasse 100 millions de dollars ou ceux qui sont considérés comme tels par le Secrétariat du Conseil du Trésor conformément à la *Politique sur les grands projets de l'État*. Lorsque les dépenses sont de cet ordre de grandeur, les projets d'EMR connexes ont tendance à être particulièrement gros et complexes. Leur portée est généralement à la fois étendue et profonde, l'objectif étant d'identifier les risques pertinents et les mesures de protection les atténuant à un niveau de détail assez granulaire. Bien que l'effort puisse être pénible, une analyse plus complète et rigoureuse s'impose généralement pour déterminer la série de mesures de sécurité la plus rentable. Comme les mesures de protection représentent habituellement de 5 % à 10 % du coût total du projet, même un petit ajustement dans les mesures de sécurité recommandées peut entraîner des économies considérables, justifiant de ce fait l'effort consacré à une évaluation officielle plus détaillée.

- **Nouvelles installations.** Chaque fois qu'une nouvelle installation doit être achetée ou construite, deux évaluations différentes peuvent être faites. La première, habituellement beaucoup plus courte, se concentre sur le profil de la menace et le profil opérationnel de l'organisation qui doit être réinstallée et vise à déterminer les critères de sécurité qui seront utilisés pour évaluer les nouveaux emplacements proposés pour l'installation. Ce projet d'EMR très ciblé, appelé **guide de sécurité du site**, contribue au choix d'un endroit qui peut être adéquatement protégé de la façon la plus efficiente et la plus rentable. Le deuxième type de projet d'EMR, qui exige normalement un effort beaucoup plus long, comprend un examen détaillé du profil de la menace et du profil opérationnel de l'organisation, ainsi que des conditions locales susceptibles de contribuer aux menaces ou aux vulnérabilités. L'objectif de cette analyse est de déterminer les mesures de sécurité matérielle souhaitables pour l'emplacement choisi. Ces recommandations, présentées sous forme de **guide de la sécurité de la conception**, peuvent être hautement conceptuelles au début d'un projet et très détaillées à la fin, selon la méthodologie de conception de l'installation. De ce fait, pour les installations plus grandes, la portée d'un projet d'EMR itératif peut être aussi étendue que pour un GPE, surtout si le processus de conception de l'installation n'a pas bénéficié d'un guide de sécurité du site.

Guide de sécurité du site
Document dans lequel sont décrits les facteurs de *sécurité matérielle* dont il faut tenir compte au moment de choisir un nouvel emplacement pour l'installation.

Guide de sécurité de la conception
Document dans lequel sont décrits les principes de base de la sécurité matérielle ainsi que les mesures de sécurité matérielle qui doivent être mises en œuvre pour chaque installation.

Guide en sécurité matérielle de la GRC G1-005
Guide pour la préparation d'un énoncé de sécurité matérielle - Janvier 2000
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

- **Nouveaux systèmes.** Évidemment, la taille et la complexité d'un système détermineront la portée de l'évaluation. Comme les biens plus complexes sont essentiellement plus vulnérables, l'analyse doit être menée à un niveau de détail plus granulaire pour que les risques éventuels soient évalués de façon plus précise. Dans le cas des systèmes en réseau, on a parfois tendance à élargir l'étendue du projet d'EMR pour couvrir tous les éléments interconnectés. Pour éviter un effort énorme et un rapport final volumineux, il est souvent préférable de subdiviser la charge de travail en plusieurs évaluations modulaires dont la portée est plus modeste, portant chacune sur un seul segment du réseau, une seule application ou une seule fonction opérationnelle, comme on peut le voir dans la figure A-1.
- **Amélioration d'une installation ou mise à niveau d'un système.** À mesure que les installations ou les systèmes évoluent, il faut mettre à jour les rapports d'EMR les concernant afin de tenir compte des changements importants en matière de sécurité. Dans ce cas, la portée de l'évaluation peut être restreinte aux variables (valeurs des biens, menaces et vulnérabilités) qui sont concrètement différentes de la configuration originale évaluée précédemment. Sauf en cas de révision ou de mise à niveau générale, l'effort de suivi pour tenir à jour les rapports d'EMR dans le cadre d'un programme global de gestion des risques peut être réduit considérablement avec un processus soigneusement structuré comme la méthodologie harmonisée d'EMR.

- **Préoccupations particulières en matière de sécurité.** Certaines des EMR les plus marquantes et les plus rentables sont celles qui visent à répondre à des préoccupations particulières en matière de sécurité, souvent un seul problème ou une seule question, comme la nécessité d'avertisseurs individuels et de vitres à l'épreuve des balles dans une cabine de service aux clients ou les exigences en matière de sécurité des émissions auxquelles doit satisfaire l'équipement utilisé à un endroit précis. Dans la plupart des cas, il est possible de restreindre énormément la portée de l'évaluation pour se concentrer sur une poignée de biens, de menaces, de vulnérabilités et de mesures de protection possibles, afin que l'analyse puisse être effectuée très rapidement et que les recommandations finales tiennent en quelques pages[2] .

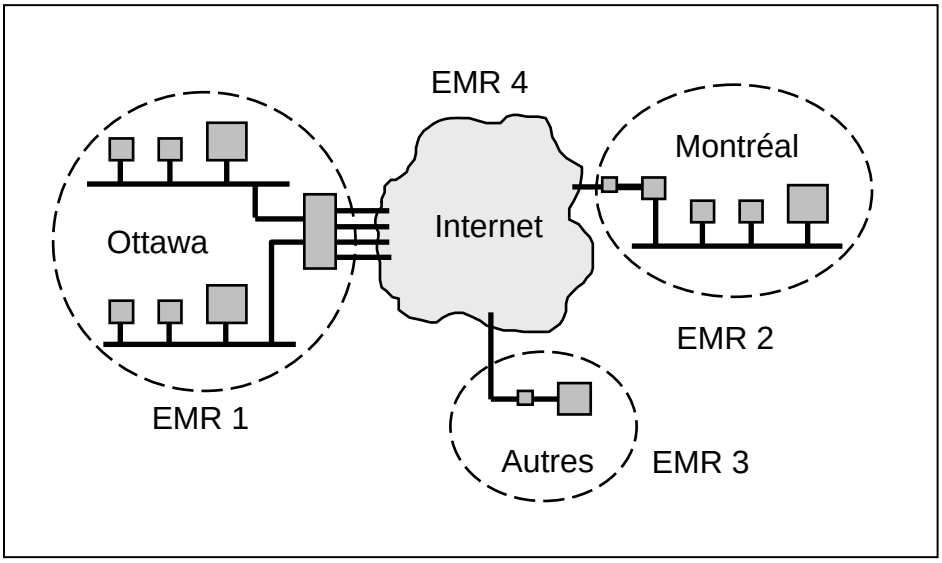

Figure A-1 : Division d'un système en réseau en projets d'EMR modulaires

4.2.3 Stade de développement

Habituellement, les projets d'installations et de systèmes évoluent, du concept initial à la définition des besoins, la conception et le développement, puis la mise en œuvre finale, conformément à un plan de projet ou à un cycle de développement de système. En règle générale, des rapports d'EMR distincts doivent être préparés à chaque étape pour soutenir une prise de décision et des choix de conception éclairés. Au départ, on en saura très peu sur les produits livrables finaux de sorte que, par la force des choses, la portée de l'évaluation préliminaire sera très générale. Cependant, à mesure que le projet avancera, et que davantage de détails seront réglés, les itérations subséquentes de l'analyse deviendront de plus en plus profondes, sinon plus étendues. Évidemment, l'ampleur du rapport d'EMR final dépendra beaucoup de la taille et de la complexité de l'installation ou du système en question. L'appendice A-1 fournit des directives plus détaillées sur l'intégration de projets d'EMR dans un projet générique ou un cycle de développement de systèmes.

[2] En fait, l'appendice F-7 présente un exemple très succinct d'un rapport d'EMR type visant à déterminer la nécessité de mesures de sécurité des émissions pour protéger une installation fictive PROTÉGÉ C au Canada.

4.2.4 Environnement de risque

Une évaluation informelle ou un examen superficiel de l'environnement de risque est souvent très utile pour mieux définir la portée d'un projet d'EMR. En général, les situations plus risquées exigent une analyse plus rigoureuse, l'objectif étant d'obtenir un niveau d'assurance plus élevé que la posture de sécurité est, effectivement, adéquate. Pour développer ce principe de base, disons que les biens qui ont plus de valeur doivent être décrits plus en détail, tout comme les menaces et les vulnérabilités plus sérieuses. Inversement, il est moins nécessaire de déployer beaucoup d'efforts pour examiner des biens qui ont moins de valeur, des menaces moins importantes ou des vulnérabilités moins évidentes. Évidemment, cela sous-entend que la granularité de l'analyse ne doit pas nécessairement être homogène à l'intérieur d'un projet d'EMR donné. Il faut toujours déployer plus d'efforts pour les questions les plus importantes, celles qui sont exposées aux plus grands risques.

4.2.5 Quelques considérations pratiques

Presque inévitablement, quelques autres considérations pratiques peuvent influer sur la portée d'une EMR. La disponibilité de normes de sécurité de base, par exemple, peut simplifier considérablement les choses, alors que les contraintes de temps, d'argent et de ressources peuvent avoir des répercussions négatives :

- **Normes de sécurité.** Dans les cas où des normes de sécurité de base fournissent des directives et des orientations adéquates pour parvenir à une posture de sécurité acceptable, il est parfois possible de raccourcir considérablement l'évaluation. Cela dit, une EMR informelle est presque toujours nécessaire pour déterminer si les normes de sécurité de base offrent une protection suffisante ou non. Plus souvent qu'autrement, les normes de sécurité existantes ne tiendront compte que d'une partie des questions, de sorte qu'un projet officiel d'EMR sera nécessaire pour combler les lacunes. Néanmoins, l'application judicieuses de diverses normes et d'autres techniques de gestion des risques étudiées à l'appendice A-2 peut aider à réduire la portée d'une évaluation et, par conséquent, la charge de travail connexe.
- **Contraintes de temps, d'argent et de ressources.** Avec une planification adéquate et le soutien de la direction, on dispose habituellement de suffisamment de temps et de ressources pour réaliser les EMR essentielles. Néanmoins, des pressions liées au calendrier et des contraintes d'argent peuvent être exercées pour diverses raisons légitimes. Par exemple, des modifications imprévues des priorités opérationnelles, de soudaines occasions d'améliorer la prestation de services, de nouvelles menaces qui évoluent rapidement et des vulnérabilités insoupçonnées jusque-là peuvent nécessiter une réaction rapide laissant trop peu de temps pour une analyse plus rigoureuse. Dans de tels cas, un évaluation à un niveau plus élevé dont la portée est plus restreinte peut devoir suffire en attendant une analyse plus détaillée lorsque le temps et les ressources le permettront. Pour obtenir les meilleurs résultats possibles, il faut concentrer le rapport de l'EMR abrégée sur les variables de risques les plus sérieuses, à savoir les biens qui ont le plus de valeur, les menaces les plus graves et les vulnérabilités les plus importantes, mais à un niveau de détail plus élevé.

4.3 Résumé

Les évaluations plus courtes sont généralement préférables aux exercices intenables de proportions massives parce qu'elles sont plus souples et plus sensibles. À cet égard, la clé du succès est de limiter la portée du projet d'EMR pour se concentrer sur l'essentiel. Les installations ou systèmes plus gros peuvent être décomposés en composants plus petits à des fins d'analyse. À l'intérieur d'une EMR donnée, le niveau de détail n'a pas besoin d'être constant, de sorte qu'on déploie moins d'efforts pour évaluer les biens qui ont moins de valeur, les menaces improbables et les vulnérabilités sans importance. Enfin, la portée d'une EMR peut changer en cours d'évaluation, à mesure que de nouvelles menaces ou vulnérabilités sont découvertes ou que de nouveaux biens sont ajoutés à l'équation.

Concrètement, la longueur d'un rapport d'EMR dépendra d'un grand nombre de variables différentes, comme la complexité des biens et des services touchés, la gravité de l'environnement de risque et le but de l'évaluation. Évidemment, le document doit être aussi long que nécessaire pour communiquer les constatations et les recommandations au responsable de l'acceptation des risques. Cela dit, le tableau A-1 donne une idée très générale de la longueur de rapports d'EMR types. Il y a toujours des exceptions, mais, dans la mesure du possible, il est préférable qu'un rapport soit plus court que long, selon l'objet de l'évaluation.

Objet du projet d'EMR	Longueur type (pages)
Évaluation ministérielle	5-10
Grand projet de l'État	100-1 000+
Nouvelle installation : Guide du site	10-20
Nouvelle installation : Guide de la conception	50-75
Nouveau système	50-100
Amélioration d'une installation ou mise à niveau d'un système	5-75
Préoccupation particulière	2-20

Tableau A-1: Longueur type des rapports d'EMR

5 Composition de l'équipe d'EMR

5.1 Généralités

Une fois la portée de l'évaluation établie, il faut réunir une équipe adéquatement qualifiée pour recueillir et analyser les données pertinentes et proposer des solutions réalistes pour satisfaire aux exigences opérationnelles. Si on ne parvient pas à bien équilibrer l'équipe, pour qu'elle représente à la fois les intérêts des opérations et les considérations relatives à la sécurité, les résultats du projet d'EMR risquent d'être biaisés, même par inadvertance, faisant état de préoccupations étriquées.

5.2 Taille de l'équipe

Il est faisable pour une seule personne d'élaborer un rapport d'EMR, mais la plupart des évaluations nécessitent un effort d'équipe pour comprendre toutes les questions, recueillir les données essentielles et obtenir des résultats en temps opportun. Voici quelques-uns des

principaux facteurs à prendre en considération au moment de déterminer la taille et la composition de l'équipe nécessaire pour réaliser un projet d'EMR précis :

- **Portée de l'évaluation**[3]**.** Les évaluations plus ciblées, particulièrement celles qui portent sur une seule question ou sur un ensemble limité de problèmes, nécessitent généralement moins de ressources, peut-être même une seule personne. Inversement, pour réaliser une évaluation exhaustive d'un grand projet de l'État dans des délais raisonnables, il peut être nécessaire de réunir une équipe beaucoup plus grosse, parfois plus de cinq spécialistes de formations différentes. Des équipes de deux ou trois personnes suffisent normalement pour les projets d'EMR qui se situent entre ces deux extrêmes, pourvu que d'autres ressources ayant des connaissances spécifiques puissent être consultées au besoin.
- **Complexité des biens.** Pour comprendre les nombreuses nuances de biens ou de processus opérationnels extrêmement complexes, il peut être nécessaire de réunir une plus grosse équipe pour disposer des connaissances et de l'expérience essentielles à une analyse efficace de la situation. Là encore, l'accès à temps partiel à des spécialistes compétents peut suffire pour réduire au minimum les exigences imposées aux rares ressources techniques.
- **Urgence de la situation.** Si le temps presse, une plus grosse équipe peut être réunie pour compléter l'analyse le plus rapidement possible. Il y a toutefois des limites pratiques, parce que les groupes plus gros peuvent être difficiles à gérer. Toute équipe comptant plus de dix membres peut devenir improductive.
- **Distribution des biens.** Si les biens sont distribués dans un grand secteur, l'équipe peut être grossie pour inclure des employés à chaque endroit pour épargner du temps de déplacement et des coûts. Dans ce cas, une coordination attentive s'impose pour assurer des résultats constants à chaque endroit.
- **Disponibilité du personnel qualifié.** Avec des employés hautement qualifiés, une plus petite équipe est normalement possible. Par contre, un soutien additionnel peut être nécessaire à plein temps ou à temps partiel pour aider des employés moins expérimentés à réaliser un projet d'EMR dans les délais prévus et au niveau de détail approprié.

5.3 Qualifications des membres de l'équipe

Pour effectuer une évaluation aussi rapidement et efficacement que possible, les membres plus expérimentés et plus avertis sont préférables aux novices. En règle générale, cependant, dans une équipe équilibrée, il faut qu'au moins un membre possède les qualifications minimales suivantes :

- une **compréhension raisonnable du processus d'EMR**, fondée sur une combinaison de formation officielle[4] et d'expérience pratique, normalement acquise après avoir participé à deux ou trois évaluations;
- une **compréhension intime des besoins opérationnels** pour les biens à l'étude, ou au moins un accès immédiat aux gestionnaires opérationnels responsables;

[3] Plusieurs facteurs qui influent sur la portée d'une évaluation sont examinés dans la **section 4.1**.

[4] Certaines des possibilités de formation sont mentionnées dans l'**avant-propos**.

- une **compréhension approfondie des normes de sécurité de base et autres mesures de protection**, ou au moins le soutien total des responsables ministériels de la sécurité, de la gestion des installations ou de la TI, dépendant du sujet de l'évaluation;
- **le niveau de pouvoir et la cote de sécurité** nécessaires pour accéder aux installations et aux renseignements pertinents.

5.4 Membres de l'équipe de base

5.4.1 Généralités

Pour respecter les qualifications minimales indiquées ci-dessus, il faut que les membres de l'équipe de base comprennent des représentants à plein temps ou à temps partiel de trois ou quatre groupes différents, selon le sujet de l'évaluation. Chacun peut apporter un point de vue important et des données clés au projet d'EMR.

5.4.2 Gestionnaires du secteur d'activité

Les gestionnaires de programme responsables du secteur d'activité à l'étude sont exceptionnellement qualifiés pour identifier tous les biens sauf les plus techniques et déterminer leur valeur en se fondant sur l'incidence opérationnelle probable d'une compromission. Comme ils comprennent la culture organisationnelle, les gestionnaires hiérarchiques sont aussi bien placés pour conseiller les cadres supérieurs sur les niveaux acceptables de risques résiduels dans les recommandations finales.

5.4.3 Gestionnaires de projet

Dans le contexte d'un projet, qu'il s'agisse d'installations ou de systèmes, les gestionnaires de projet et les membres de leur personnel peuvent identifier les biens plus techniques, un grand nombre de leurs vulnérabilités, les mesures de protection proposées et les solutions de rechange éventuelles au besoin. Leur contribution aux recommandations et leur accord global avec les propositions sont essentiels à la réussite du rapport d'EMR.

5.4.4 Gestionnaires des installations

Dans les projets d'EMR touchant les édifices gouvernementaux et d'autres travaux publics, les gestionnaires des installations peuvent identifier les biens structurels et environnementaux, les menaces locales en se fondant sur les rapports des gardes et les enregistreurs de signaux d'alarme, certaines vulnérabilités techniques associées à la structure de l'immeuble et à son emplacement, et un grand nombre de mesures de sécurité matérielle. Souvent, ils peuvent fournir des dessins architecturaux et des plans d'étage pour aider à délimiter la portée de l'évaluation, illustrer de nombreux biens sur place et faciliter l'analyse subséquente de solutions de rechange adéquates en prévision des recommandations finales.

5.4.5 Responsables des TI

Au niveau stratégique, les dirigeants principaux de l'information (DPI) et les membres de leur personnel peuvent identifier les biens des TI, particulièrement l'infrastructure sous-jacente et d'importants liens avec d'autres systèmes. D'un point de vue plus tactique, les contributions des administrateurs des systèmes peuvent être particulièrement précieuses, allant de descriptions de plus en plus détaillées des biens des TI et de leur configuration concrète, aux menaces réelles

compte tenu des données consignées dans les journaux d'exploitation, des vulnérabilités connues ou présumées et des mesures de protection techniques actuelles.

5.4.6 Responsables de la sécurité

La PGS et les documents à l'appui exigent que les ministères nomment trois conseillers principaux en matière de sécurité, à savoir un agent de sécurité du ministère (ASM)[5], un coordonnateur de la sécurité des TI (CSTI)[6] et un coordonnateur de la planification de la continuité des activités (CPCA)[7]. Les ASM et les membres de leur personnel peuvent contribuer concrètement à presque toutes les EMR, alors que les CSTI devraient participer à toutes celles qui touchent les biens des TI, et les CPCA, à celles qui touchent des biens ou services essentiels. Plus précisément, ces responsables assurent le soutien suivant :

- **ASM** – interprète la PGS et les documents à l'appui à l'intention du ministère, fournit aide et conseils sur le processus d'EMR en général, contribue aux évaluations des menaces et des vulnérabilités en se fondant sur les rapports d'incidents et les enquêtes internes et propose des mesures de protection adéquates en vue des recommandations finales.
- **CSTI** – interprète les normes de sécurité des TI à l'intention du ministère, offre son point de vue sur les menaces et les vulnérabilités techniques et propose des mesures de protection techniques adéquates en vue des recommandations finales.
- **CPCA** – interprète les normes du programme de PCA à l'intention du ministère, peut fournir des analyses des répercussions sur les opérations (ARO) pertinentes pour identifier les biens et services essentiels, offre son point de vue sur les menaces et les vulnérabilités qui peuvent avoir une incidence sur ces biens et services et propose des mesures, des ententes et des plans de continuité des activités adéquats, s'il y a lieu, pour les recommandations finales.

5.4.7 Coordination globale

Selon l'objet du projet d'EMR, n'importe lequel des principaux membres de l'équipe peut coordonner l'évaluation globale, mais chacun aura une orientation différente. Les gestionnaires de programmes sont plus susceptibles de se concentrer sur les exigences opérationnelles, une considération prépondérante. Les gestionnaires de projet sont souvent motivés par les contraintes d'argent et de calendrier et peuvent, par conséquent, remettre en question la nécessité de mesures de protection coûteuses. Les responsables des TI, y compris le CSTI, ont une meilleure compréhension d'un grand nombre de questions techniques, mais peuvent perdre de vue les mesures de sécurité du personnel et de sécurité matérielle, si importantes dans les solutions exhaustives. Inversement, l'ASM a une vaste compréhension de tout le programme de sécurité ministériel, mais pas nécessairement la profondeur technique pour certaines évaluations de sécurité des TI. Tous ces facteurs doivent être pris en considération au moment de choisir un chef d'équipe, mais la question la plus importante est celle de l'impartialité : pour satisfaire à

---

5 La **section 10.1 de la PGS** exige la nomination d'un ASM.

6 La **section 9.1 de la *Norme sur la gestion de la sécurité des technologies de l'information* (GSTI)** exige la nomination d'un CSTI.

7 La **section 3.1 de la *Norme opérationnelle de sécurité - Programme de planification de la continuité des activités* (PCA)** exige la nomination d'un CPCA.

leurs obligations aux termes de la PGS et de la fonction moderne de contrôleur, les administrateurs généraux et les membres de leurs équipes de direction ont besoin d'évaluations objectives qui peuvent résister même à un examen minutieux du public et prouver que toutes les précautions voulues ont été prises si une menace devait se concrétiser et compromettre des biens de valeur. Compte tenu de cela, le bureau de l'ASM, à titre de tiers impartial, doit collaborer étroitement avec le chef d'équipe désigné pour surveiller la qualité et l'exhaustivité de l'analyse et fournir des conseils à cet égard.

5.5 Autres ressources

5.5.1 Ressources internes

Il est possible de consulter beaucoup d'autres ressources ministérielles au cours d'un projet d'EMR pour obtenir des renseignements spécialisés, des conseils et de l'aide au besoin :

- **Coordonnateurs de l'AIPRP** – pour aider à déterminer la valeur des biens, surtout les aspects relatifs à l'accès à l'information et à la protection des renseignements personnels lorsqu'il est question de biens liés à l'information et, s'il y a lieu, fournir des copies des évaluations des facteurs relatifs à la vie privée (EFVP) pertinentes dans un but semblable.
- **Finances** – pour aider à identifier les biens financiers et à en déterminer la valeur, ainsi que les pertes signalées à l'État conformément aux politiques du Conseil du Trésor[8], à titre d'indicateurs possibles de la menace.
- **Ressources humaines** – pour expliquer les questions relatives au personnel, identifier les employés exposés à des risques de violence et proposer les préoccupations relatives aux relations de travail qui pourraient révéler l'existence de menaces ou vulnérabilités internes.
- **Vérification interne** – pour discuter des vérifications et examens ministériels portant sur le respect des politiques et des normes de sécurité en tant que mesure de l'efficacité et de la vulnérabilité des mesures de protection.
- **Conseillers juridiques** – pour interpréter les obligations juridiques et les responsabilités et, dans les situations particulièrement délicates, examiner les EMR afin d'évaluer si elles documentent adéquatement la diligence raisonnable.
- **Gestion du matériel** – pour identifier certains biens matériels et leur valeur en se fondant sur les fiches d'inventaire.
- **Santé et sécurité au travail** — pour fournir de l'information sur les risques en milieu de travail à l'étape de l'évaluation des menaces et proposer des mesures de protection pertinentes en vue des recommandations.

[8] La ***Politique sur les pertes de deniers et infractions et autres actes illégaux commis contre la Couronne*** exige que les ministères fassent enquête et signalent toutes les pertes de fonds et les allégations d'infractions, d'actes illégaux contre la Couronne et autres actes irréguliers, qui sont autant d'indicateurs utiles d'activités liées à la menace.

5.5.2 Ressources externes

Parmi les ressources externes susceptibles d'être utiles à une équipe d'EMR mentionnons les suivantes :

- **Organismes conseils en matière de sécurité** désignés par le SCT[9], plus particulièrement —
    - **le CST** – pour obtenir aide et conseils sur la méthodologie harmonisée d'EMR et les menaces techniques, les vulnérabilités et les mesures de protection touchant les systèmes de TI.
    - **le SCRS** – pour une évaluation des menaces définies dans la *Loi sur le SCRS*.
    - **SPPCC** – pour obtenir aide et conseils sur la planification de la continuité des activités et la protection des infrastructures essentielles, ce qui comprend les alertes, les avis et les notes d'information sur les menaces possibles, imminentes ou réelles, les vulnérabilités ou les incidents qui touchent le gouvernement du Canada ou d'autres secteurs des infrastructures essentielles nationales.
    - **TPSGC** – pour obtenir aide et conseils sur la sécurité des systèmes de TI et des installations pour lesquels il est le fournisseur de services commun et dont il a la garde, respectivement.
    - **la GRC** – pour obtenir aide et conseils sur la méthodologie harmonisée d'EMR, toutes les questions liées à la sécurité matérielle, aux menaces criminelles et aux menaces techniques, les vulnérabilités et les aspects opérationnels de la sécurité des TI.
- **Autres organismes du secteur public**, comme les services de police provinciaux et municipaux, les services d'incendie et les services publics, qui peuvent fournir des renseignements précieux sur les biens environnementaux, les menaces locales et certaines vulnérabilités, comme on peut le voir dans les appendices B-1, C-1 et D-1, respectivement.
- **Organismes du secteur privé**, comme l'industrie de l'assurance, les fournisseurs de produits, les associations professionnelles et les instituts de recherches, qui peuvent aussi fournir des renseignements précieux sur divers biens, menaces, vulnérabilités et mesures de protection, comme il est indiqué dans les appendices B-1, C-1, D-1 et F-1, respectivement.
- **Consultants du secteur privé**, qui peuvent être engagés à contrat pour leur expertise technique pour compléter les ressources ministérielles ou même pour réaliser des projets d'EMR complets. Le recours à des consultants offre plusieurs avantages, mais peut aussi causer quelques problèmes. L'appendice A-4 étudie un grand nombre de ces questions plus en détail et présente certaines des pratiques exemplaires pour obtenir des résultats plus constants. L'appendice A-5 fournit un exemple d'énoncé des travaux pour les services de consultants en EMR qui pourra servir de modèle aux ministères.

[9] La **section 4 de l'appendice A de la PGS** fournit une description plus complète des rôles et responsabilités de tous les ministères responsables en matière de sécurité.

6 Plan de travail de l'EMR

Sauf dans le cas des évaluations les plus courtes et les plus simples, la plupart des projets d'EMR bénéficieront considérablement d'un plan de travail officiel. La longueur et le niveau de détail exacts varieront en fonction de la portée et de la complexité de l'évaluation, mais un plan de travail type doit comprendre :

- quelques **données de base** pour situer l'évaluation dans le contexte ministériel;
- l'**objectif** ou le but clairement énoncé du projet d'EMR, généralement en une seule phrase;
- un énoncé de la **portée** précisant le sujet de l'évaluation et les limites de l'analyse;
- toute **limite** ou restriction de l'EMR, comme les contraintes de temps ou d'argent;
- le **niveau de risque maximal** jugé acceptable;
- la **composition de l'équipe** ainsi que des mandats pour chacun des membres;
- toutes les **dispositions logistiques** comme —
    - les besoins en matière de filtrage de sécurité,
    - les besoins d'accès aux installations et aux données, tant matériels que logiques,
    - les préparatifs de voyage et plans de visites,
    - le soutien administratif,
    - les autres besoins en ressources (locaux, matériel de bureau),
    - un budget ventilé,
    - les énoncés des travaux des services de consultants (s'il y a lieu);
- une liste de **documents de référence** possibles, comme des documents conceptuels, des plans des installations, des PE sur le partage des renseignements et d'autres biens et les rapports des EMR antérieures[10];
- les résultats prévus ou **produits livrables**, précisant la méthodologie d'EMR à employer, le format des copies papier et électronique du rapport d'EMR final et les voies à suivre pour le présenter;
- le **calendrier** du projet, dressant la liste des activités avec les dates de début et d'achèvement de chaque phase de l'évaluation et tous les produits livrables connexes.

7 Approbation

En général, le cadre supérieur qui examinera les recommandations de l'EMR doit approuver le plan de travail avant que l'équipe soit réunie et que la collecte des données commence.

Enfin, l'appendice A-6 présente un exemple de plan de travail de l'EMR avec des instructions détaillées pour l'établir.

[10] Des listes plus complètes des sources possibles de données sont présentées dans les appendices B-1 pour les biens, C-1 pour les menaces, D-1 pour les vulnérabilités et F-1 pour les mesures de protection.

Page intentionnellement laissée en blanc

Appendice A-1 – Les EMR dans un plan de projet/cycle de vie d'un système

1 Introduction

1.1 Généralités

Un seul projet d'EMR suffit pour évaluer les risques associés à des installations, des systèmes ou des services existants. Toutefois, si les responsables ont omis de prendre en compte les préoccupations en matière de sécurité au cours du développement, plusieurs des risques résiduels calculés durant la Phase d'évaluation des risques peuvent s'avérer inacceptables et mener à la recommandation de propositions de mesures correctives complexes et souvent coûteuses lors de la Phase des recommandations.

Pour contourner les difficultés liées au réajustement des mesures de protection des biens existants, on doit effectuer des évaluations itératives des menaces et des risques à chaque étape du plan de projet ou du cycle de vie d'un système. Cette approche facilite l'identification précoce des risques potentiellement dangereux et la détermination d'alternatives de conception raisonnables qui permettent d'atteindre les objectifs opérationnels en recourant aux solutions de sécurité les plus rentables.

1.2 But

Le but de cet appendice est d'offrir certaines directives concernant l'intégration de rapports d'EMR dans un plan de projet ou le cycle de vie d'un système.

2 Stades d'un plan de projet/cycle de vie d'un système

2.1 Options de planification de projet

Tous les grands projets de remaniement de processus opérationnel et de conception d'installation ou de système devraient suivre des phases ou stades séquentiels, de la conceptualisation initiale au déploiement opérationnel (et même au retrait final). Différentes disciplines professionnelles ont défini des modèles distincts mais fondamentalement similaires de planification de projet et de développement de système. Voici quelques exemples particuliers :

- plusieurs cycles de vie de projet représentatifs sont proposés dans le document *Project Management Body of Knowledge (PMBOK®)*;
- un processus de conception de système de sécurité est décrit à la section 1.2 et la figure 2 du document G1-005, *Guide pour la préparation d'un énoncé de sécurité matérielle*, publié par la GRC; et

- un cycle de vie de système générique fait l'objet d'un examen à la section 2.1.1 du document MG-2, *Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information*, publié par le CST.

2.2 Cycle de vie de projet

Un des cycles de vie de projet représentatifs mentionnés dans le document *Project Management Body of Knowledge (PMBOK®)* pour l'acquisition de moyens de défense inclut les quatre phases suivantes :

- **Développement du concept et de la technologie** – études préliminaires fondées sur le concept d'opération pour la sélection d'une architecture de système;
- **Développement et démonstration du système –** développement, intégration et démonstration du système dans un environnement opérationnel;
- **Production et déploiement –** fabrication et installation complètes; et
- **Soutien –** gestion et ajustement continus.

2.3 Processus de conception d'installation

Dans le document G1-005, *Guide pour la préparation d'un énoncé de sécurité matérielle*, la GRC décrit un processus de conception de système de sécurité en six étapes pour les installations gouvernementales :

- **Planification –** définition des besoins opérationnels et d'une stratégie de protection;
- **Détermination –** analyse des attributs du site et de l'installation conformément à la stratégie de protection;
- **Mise en œuvre –** conception de l'installation et mise en place des mesures de protection pour assurer le respect de la stratégie de protection;
- **Mise en service –** inspection de l'installation pour assurer le respect de la stratégie de protection;
- **Fonctionnement –** surveillance des opérations pour assurer le respect continu; et
- **Évaluation –** évaluation du projet en fonction des critères de rendement et rajustement approprié des mesures de protection.

2.4 Cycle de vie d'un système

Dans le document MG-2, *Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information*, le CST présente un cycle de vie à six stades :

- **Planification des modifications –** examen des divers programmes possibles et des risques connexes, et décision concernant la pertinence de lancer ou non le projet;
- **Définition des exigences –** détermination des besoins opérationnels et exigences fonctionnelles de sécurité connexes;
- **Spécifications générales –** identification des options de systèmes sûrs et sélection de l'architecture préférée;

- **Spécification détaillées –** développement des spécifications de conception et de mesures de protection précises pour satisfaire à la politique de système de sécurité et aux exigences fonctionnelles;
- **Mise en œuvre –** achèvement des activités d'acquisition, d'installation et de test; et
- **Exploitation –** commencement des opérations, incluant les activités continues de maintenance et d'examen pour conserver la posture de sécurité.

2.5 Résumé

Quoiqu'il existe beaucoup plus de modèles de planification de projet ou d'installation et de développement de système, les trois exemples décrits précédemment illustrent le flux logique, de l'analyse des options de haut niveau jusqu'aux activités de plus en plus détaillées de définition des exigences, de conception, de développement, de test et de déploiement opérationnel. Le tableau A1-1 souligne les relatives similarités entre ces processus.

<table>
<tr><th>Cycle de vie de projet</th><th>Processus de conception d'installation</th><th>Cycle de vie d'un système</th></tr>
<tr><td rowspan="2">Développement du concept et de la technologie</td><td>Planification</td><td>Planification des modifications</td></tr>
<tr><td rowspan="3">Détermination</td><td>Définition des exigences</td></tr>
<tr><td rowspan="2">Développement et démonstration du système</td><td>Spécifications générales</td></tr>
<tr><td>Spécifications détaillées</td></tr>
<tr><td rowspan="2">Production et déploiement</td><td>Mise en œuvre</td><td rowspan="2">Mise en œuvre</td></tr>
<tr><td>Mise en service</td></tr>
<tr><td rowspan="2">Soutien</td><td>Fonctionnement</td><td rowspan="2">Exploitation</td></tr>
<tr><td>Évaluation</td></tr>
<tr><th colspan="3">Documents sources</th></tr>
<tr><td>A Guide to the Project Management Body of Knowledge (PMBOK ® Guide)</td><td>G1-005, Guide pour la préparation d'un énoncé de sécurité matérielle</td><td>MG-2, Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information</td></tr>
</table>

Tableau A1-1 : Stades relatifs à un plan de projet ou à un cycle de vie d'un système

3 Conséquences pour les rapports d'EMR

3.1 Justification

Quelle que soit la méthodologie de planification de projet ou de cycle de vie d'un système sélectionnée pour gérer la conception et le déploiement d'une nouvelle installation, d'un nouveau système ou d'un nouveau service, certains principes fondamentaux doivent gouverner les activités d'EMR sous-jacentes. En fait, sans une relation clairement définie entre le projet et les fonctions de gestion des risques de sécurité, il est possible que l'on ne tienne pas compte de la gravité de certaines menaces et vulnérabilités, que l'on néglige des mesures de protection

essentielles et, ainsi, que l'on s'expose, sans les reconnaître, à des risques résiduels inacceptables. Toute tentative de corriger des défauts de sécurité après l'occupation d'une nouvelle installation ou la mise en place d'un système est susceptible d'échouer ou, du moins, d'entraîner des coûts exorbitants.

3.2 Principes de base

3.2.1 Intervention dès le stade initial

Dans un premier temps, d'abord et avant tout, les processus d'EMR doivent être enclenchés dès les premières phases d'un projet, c.-à-d., au stade de la conception ou de la planification. Évidemment, la première évaluation sera un examen de haut niveau puisque plusieurs biens et leurs vulnérabilités connexes ne peuvent être identifiés avant les activités de conception détaillée qui seront entreprises plus tard au cours du cycle de vie du projet. Néanmoins, le premier rapport d'EMR peut influencer l'orientation d'un projet; il peut contribuer à l'identification et au rejet des options ou alternatives dont les risques sont plus élevés.

3.2.2 Analyse itérative

Au cours de chaque stade successif du plan de projet ou du cycle de vie d'un système, davantage de détails seront recueillis sur les biens, leurs valeurs, les menaces et les vulnérabilités connexes. Il sera alors possible d'évaluer le risque résiduel avec plus de précision et de certitude à chaque étape du processus, tel qu'il est illustré à la figure A1-1.

3.3.3 Approbation provisoire

L'objectif des rapports intérimaires d'EMR est d'identifier les risques résiduels potentiellement inacceptables et de suggérer des solutions de sécurité rentables avant que l'équipe de projet n'arrête irrévocablement ses choix de conception. Tant les gestionnaires de projet que de programme devraient examiner et approuver les recommandations de chaque rapport successif d'EMR, ou demander des propositions de solutions de rechange satisfaisantes.

3.3 Avantages potentiels

Les avantages de méthodologies étroitement intégrées de planification de projet, de développement de système et de gestion des risques incluent une meilleure assurance de la prise de décisions responsables, avec une piste de vérification visible et des justifications claires des choix de conception témoignant d'une diligence raisonnable au cas où se matérialiseraient des risques.

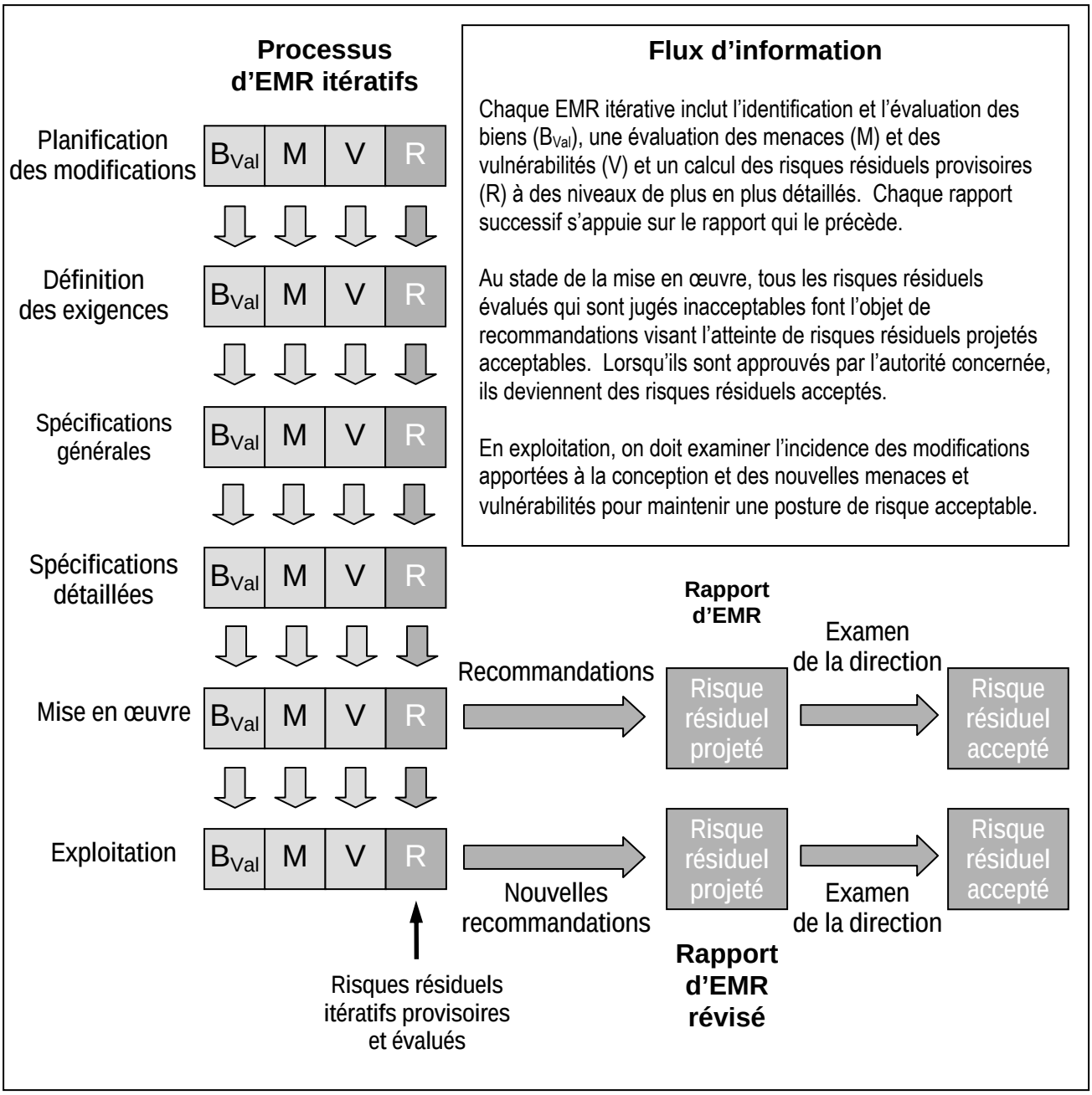

Figure A1-1: Flux d'information d'EMR dans un environnement de projet

Page intentionnellement laissée en blanc

Appendice A-2 - Normes de sécurité et évaluations des menaces et des risques

1 Introduction

1.1 Exigences de la *Politique du gouvernement sur la sécurité* (PGS)

Au plus haut niveau d'abstraction, la gestion des risques n'est rien de plus qu'une réponse systématique à l'incertitude. Du point de vue de la sécurité, cette incertitude résulte de l'interaction de plusieurs variables indépendantes dont certaines sont particulièrement difficiles à évaluer. Plus précisément, la gestion des risques dans un contexte de sécurité est une tentative de traiter les conséquences négatives d'un agent de menace qui exploite une vulnérabilité donnée pour porter préjudice à un bien de valeur. Essentiellement, on peut décrire le risque (**R**) comme une relation fonctionnelle entre les valeurs d'un bien ($\mathbf{B_{Val}}$), les menaces (**M**) et les vulnérabilités (**V**) :

$$\mathbf{R = \mathit{f}\ (B_{Val}, M, V)}$$

Même si cette relation fonctionnelle est largement acceptée, la gestion des risques a fait l'objet d'un débat passionné dans les cercles de responsables de la sécurité. Différentes communautés d'intérêts ont épousé différentes approches analytiques. Certaines, par exemple, ont préféré des techniques qualitatives alors que d'autres ont recherché des mesures quantitatives. Certaines encore ont appuyé des solutions fondées sur des règles et d'autres ont effectué des études de cas. Malgré une abondance de discussions informées et de recherches documentées, aucune approche particulière n'a été choisie unanimement par les professionnels de la sécurité.

Même si la variété des options peut offrir une souplesse intéressante, un trop grand nombre de choix est susceptible d'engendrer la confusion. Pour réduire l'incertitude et établir des approches communes au sein des ministères et organismes fédéraux, la *Politique du gouvernement sur la sécurité* prescrit donc deux options de gestion des risques dans l'énoncé suivant :

> « On doit sauvegarder les biens selon des exigences sécuritaires de base et une gestion continue des risques pour la sécurité. »[1]

Dans l'Appendice B de la politique, le Glossaire, les « exigences sécuritaires de base » sont définies comme suit : « dispositions obligatoires de la *Politique du gouvernement sur la sécurité*, de ses normes opérationnelles et de sa documentation technique. » La section 9 de la politique élabore davantage et décrit la hiérarchie des documents à l'appui de la politique alors que l'Appendice A attribue, aux ministères désignés responsables de la sécurité, des responsabilités précises pour le développement des normes de sécurité tant opérationnelles que techniques.

[1] **Section 4 de la PGS**.

Au plan de la gestion des risques de sécurité, la politique charge les ministères d'« effectuer des évaluations des menaces et des risques pour déterminer la nécessité d'aller au-delà des mesures sécuritaires de base. »[2] Elle définit un processus d'évaluation des menaces et des risques (EMR) en quatre étapes à l'appui de cette directive. L'Appendice A identifie également les organismes conseils et énumère leurs responsabilités particulières pour ce qui est des conseils et directives touchant à la fois le processus d'EMR et les données nécessaires à l'exécution d'une évaluation. Enfin, la documentation connexe, plus particulièrement les Normes opérationnelles de sécurité sur l'identification des biens et la gestion des risques de sécurité, donne davantage de détails sur cette approche particulière de gestion des risques.

La PGS identifie clairement l'EMR comme complément important des normes de sécurité de base d'un programme intégré de gestion des risques; toutefois, des directives supplémentaires sur les mérites relatifs des deux méthodes et de leur application dans des circonstances différentes peuvent être utiles. En même temps, d'autres options peuvent justifier que l'on s'y attarde.

1.2 But

Le but de cet appendice a trois volets :

- décrire les différentes options d'une gestion des risques rationnelle et responsable;
- évaluer les forces et faiblesses relatives de chaque approche; et
- proposer des situations ou des circonstances spécifiques où chaque technique est plus appropriée.

2 Approches de gestion des risques

2.1 Généralités

Bien que la variété des méthodologies de gestion des risques soit potentiellement illimitée, plusieurs options sont essentiellement semblables ou simplement des variations d'un même thème. En vue d'obtenir un cadre significatif d'analyse, on identifie deux caractéristiques sous-jacentes pour établir une distinction entre quatre techniques différentes. La complexité analytique d'un outil de gestion des risques déterminera l'expertise relative nécessaire pour compléter une évaluation, ainsi que la durée et les coûts de l'effort. D'autre part, l'application de certaines approches est plus intuitive ou subjective alors que la nature d'autres approches est plus objective. À partir de ces caractéristiques distinctes, le reste de cet appendice examine quatre méthodes différentes illustrées dans la figure A2-1 : EMR non officielle ou superficielle, recours à des spécialistes compétents, application de normes de sécurité et EMR intégrée ou officielle. La PGS reconnaît et appuie intégralement les deux dernières méthodes seulement.

[2] **Section 10.7 de la PGS**.

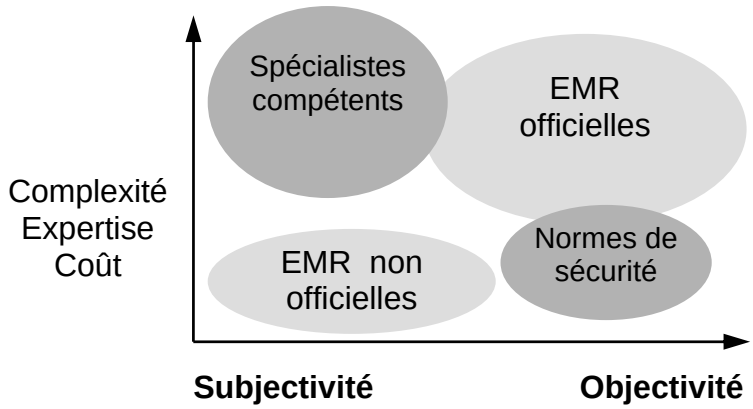

Figure A2-1: Méthodologies de gestion des risques

2.2 Évaluation non officielle des menaces et des risques

Intuitivement, les êtres humains prennent régulièrement des décisions importantes, voire critiques, concernant leur sécurité personnelle et leur bien-être. Que ce soit des situations simples, par exemple traverser une rue passante, ou des problèmes plus complexes concernant leur sécurité financière ou des soins de santé, les individus évaluent les risques et adoptent une ligne de conduite. Ils font souvent ces choix très rapidement, presque inconsciemment, avec un minimum d'analyse formelle.

Au premier coup d'œil, cette approche minimaliste de la gestion des risques peut sembler complètement irresponsable, laissant deviner une certaine inconscience ou même une réticence à reconnaître les menaces et vulnérabilités réelles. Cela est presque certainement le cas lorsque le choix est fait de manière inconsciente ou totalement arbitraire. Toutefois, une telle logique intuitive peut être parfaitement raisonnable lorsque les risques réels sont relativement faibles, c'est-à-dire lorsque les valeurs des biens ou les vulnérabilités connexes sont modestes et que les menaces connexes sont soit inexistantes ou au moins très improbables.

Par exemple, un gestionnaire de risque consciencieux, après avoir effectué seulement une analyse limitée, peut ne pas tenir compte des mesures de protection contre les inondations lorsqu'une installation gouvernementale est située en haut d'une colline. Les connexions étendues d'Internet aux réseaux ministériels offrent toutefois des exemples moins futiles. En dépit des menaces et des vulnérabilités connues, ces liens peuvent être entièrement justifiés lorsque les préoccupations au plan de la confidentialité, de la disponibilité et de l'intégrité sont très faibles. En résumé, une approche non officielle de la gestion des risques fondée sur une EMR superficielle peut être parfaitement acceptable et entièrement raisonnable lorsque les conditions s'y prêtent et que les risques connus ne justifient pas les dépenses et les efforts supplémentaires que nécessite un analyse plus rigoureuse.

2.3 Spécialistes compétents (sagesse de Delphes)

Selon l'ancienne mythologie grecque, l'oracle de Delphes pouvait communiquer aux simples mortels des directives et des conseils judicieux. Malheureusement, ces prophéties étaient fréquemment obscures, ambiguës ou énigmatiques et, par conséquent, pouvaient être mal interprétées ou appliquées.

Si l'on établit un parallèle avec notre monde moderne, même les conseils le plus sages d'experts en sécurité reconnus peuvent être tout aussi incompréhensibles pour le non initié. Trop souvent, hélas, les rapports sont truffés de jargon technique et de détails obscurs, dont certains peuvent être source de confusion pour les responsables de programmes.

Malgré ces difficultés, l'expérience actuelle des vrais enjeux et des problèmes pratiques peut servir de base solide à une gestion efficace des risques. Bien qu'un conseiller chevronné puisse suffire à la tâche, le niveau de confiance à l'égard d'une solution proposée est susceptible de s'accroître de manière significative lorsque des spécialistes compétents participent à l'évaluation des exigences de sécurité et à la proposition de mesures de protection viables. Le produit de ces délibérations est presque toujours présenté dans un rapport écrit, normalement sous forme d'évaluation narrative, qui formule des recommandations spécifiques. Même si la nature du résultat est généralement subjective, la plupart des professionnels incluent dans ces rapports une variété de documents justificatifs sous forme de données, de graphiques, de tableaux et de modèles de coûts pour justifier les mesures de sécurité proposées.

2.4 Normes de sécurité

Les normes de sécurité imposées par la *Politique du gouvernement sur la sécurité* figurent dans un ensemble de documents accessoires mentionnés à la section 9 de la PGS. Cette référence importante est étayée à la section 2 de la Norme de sécurité relative à l'organisation et l'administration, qui décrit à la fois la structure des documents, illustrée dans la figure A2-2, ainsi qu'un processus détaillé de développement, d'approbation et de promulgation. La structure hiérarchique s'avère particulièrement pratique et logique compte tenu que le domaine de la sécurité est simplement trop difficile à définir dans une seule politique, si volumineuse et lourde soit-elle. Un éventail de publications de plus en plus détaillées, de la PGS actuelle aux six normes opérationnelles et à une véritable bibliothèque de documentation technique, constitue une approche plus pratique et réaliste pour les normes de sécurité de base actuelles.

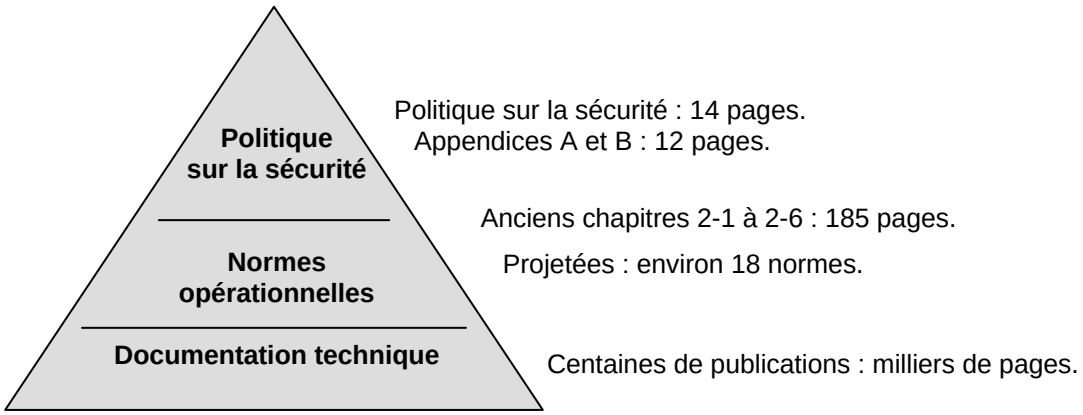

Figure A2-2: Structure des documents sur la sécurité

Au sein du gouvernement fédéral, trois organismes responsables (le Centre de la sécurité des télécommunications [CST], Sécurité publique et Protection civile Canada [SPPCC] et la Gendarmerie royale du Canada [GRC]) ont été chargés de responsabilités précises concernant l'élaboration de normes techniques sur la sécurité matérielle et des TI et sur la planification de la continuité des activités.

En général, ces normes prescrivent certaines mesures de protection, ou combinaisons de mécanismes de protection, pour des biens particuliers, selon leur valeur et, dans une moindre mesure, leur environnement de menace et leur vulnérabilité. Le calendrier recommandé pour le changement des mots de passe est un exemple simple d'une telle mesure, soit un changement mensuel pour l'accès à l'information classifié Très secret, un changement trimestriel pour l'information classifiée Secret et Confidentiel et un changement biannuel pour l'information protégée (anciennement désignée).[3] En fait, le caractère graduel de ces interventions se fonde uniquement sur la valeur du bien, sans égard à ses vulnérabilités ni à son environnement de menace immédiat. D'autres normes, comme celles concernant les domaines de la sécurité matérielle et des TI, offrent un éventail de mesures de protection techniques pour traiter des vulnérabilités opérationnelles croissantes. De tels compromis sont des éléments courants de nombreuses normes de sécurité.

2.5 Évaluation officielle des menaces et des risques

Une évaluation officielle des menaces et des risques est une alternative viable à l'application simple des normes de sécurité. Tel qu'il a été défini à un niveau supérieur d'abstraction dans la Norme de sécurité relative à l'organisation et l'administration, ce processus qui semble relativement simple et intuitivement satisfaisant comprend quatre étapes de base :

- **Planification initiale et énoncé de sensibilité** – établissement de la portée de l'évaluation et identification des employés et des biens à protéger.

3 **Section 8.2(6) de la *Norme de sécurité technique dans le domaine de la technologie de l'information (NSTTI)*** publiée antérieurement par la GRC et disponible au site suivant : http://www.rcmp-grc.gc.ca/tsb/pubs/it_sec/tssit97_f.pdf

- **Évaluation des menaces** – détermination des menaces aux employés et aux biens au Canada et à l'étranger, et évaluation de la probabilité et de l'incidence de l'occurrence d'une menace.
- **Évaluation des risques** – évaluation des risques fondée sur la pertinence des mesures de protection existantes et des vulnérabilités.
- **Recommandations** – mise en œuvre de toute mesure de protection supplémentaire permettant de réduire les risques à un niveau acceptable.

Chaque étape n'est toutefois pas un exercice futile et les organismes responsables ont élaboré un éventail de documents mettant en relief les dispositions fondamentales de la PGS et de la Norme opérationnelle de sécurité de la gestion des risques pour la sécurité; la majorité de ces documents a été remplacée par la *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)*. Des publications similaires abondent dans le secteur privé, de même que de nombreux outils automatisés qui aident à définir une approche structurée pour la collecte et l'analyse de données pertinentes.

3 Mérites relatifs

3.1 Généralités

Chaque approche de gestion des risques possède ses propres forces et faiblesses, héritées de leur relative complexité, leurs coûts de mise en œuvre, leur pertinence et leur disponibilité dans différentes circonstances. Il est essentiel de posséder une connaissance de base de ces différents aspects pour prendre des décisions éclairées concernant la méthodologie particulière la mieux adaptée à une situation précise.

3.2 Évaluation non officielle des menaces et des risques

3.2.1 Avantages

De toute évidence, l'EMR non officielle ou superficielle offre plusieurs avantages importants puisqu'elle est de loin la plus simple. Presque invariablement, elle est la plus facile à appliquer et celle qui prend le moins de temps et, de ce fait, elle permet de réduire les coûts et les demandes imposées aux rares spécialistes de la sécurité. Malgré une analyse superficielle, ses résultats peuvent être très précis et entièrement reproductibles lorsqu'ils sont appuyés par un processus précis et de haut niveau d'énoncé de sensibilité et d'évaluation des menaces.

3.2.2 Inconvénients

Pour éviter des mesures de protection coûteuses, certains gestionnaires ont été tentés d'appliquer des techniques non officielles à des situations pour lesquelles elles sont inappropriées, et même dangereuses, et où existent des risques vraiment importants qui ne peuvent être ignorés. En résumé, une application inappropriée de cette méthode et une représentation erronée de ses résultats représentent les plus grands dangers ou inconvénients d'une méthodologie minimaliste. Les lacunes au plan de la documentation des décisions importantes sont susceptibles de créer d'autres problèmes. Sans une documentation officielle, il peut être difficile de démontrer que l'on a été responsable et que l'on a fait preuve d'un diligence raisonnable advenant une sérieuse

brèche de sécurité. Enfin, en raison de sa nature même, une approche minimaliste offre peu d'analyse pour justifier tout investissement réel dans des mécanismes de protection; elle se prête bien uniquement à des cas isolés ou à des situations relativement simples.

3.3 Spécialistes compétents

3.3.1 Avantages

Malgré que la consultation et la rédaction de rapport inhérentes à cette approche soient laborieuses, les professionnels de la sécurité plus expérimentés répondent en général très rapidement à la plupart des exigences. Évidemment, le niveau d'effort requis est facilement adapté pour tenir compte de presque tous les échéanciers, budgets opérationnels et configurations de biens et pour proposer des recommandations ciblées de manière rentable. Habituellement, les rapports écrits offrent une piste de vérification acceptable aux fins de la reddition de compte.

3.3.2 Inconvénients

À l'occasion, la rareté de spécialistes compétents peut constituer un réel obstacle, plus particulièrement pour ce qui touche les plus récentes technologies ou les systèmes et les installations plus complexes, puisqu'un moins grand nombre de ces professionnels a eu la possibilité d'acquérir les connaissances requises. Ce problème peut être particulièrement grave dans les situations qui nécessitent des niveaux d'assurance supérieurs, où la prudence exige d'obtenir des données de deux sources ou plus afin de corroborer les constatations et les recommandations. La subjectivité même de l'analyse pose un autre problème potentiel puisque les résultats peuvent varier considérablement selon les connaissances et l'expérience personnelles des analystes concernés. La reproductibilité peut être difficile à atteindre, ce qui peut avoir de graves incidences sur l'interopérabilité et la crédibilité même du processus. Les conséquences peuvent être sérieuses si les solutions recommandées sont particulièrement coûteuses ou onéreuses. Sans mesures plus objectives qu'un rapport narratif, les résultats peuvent être remis en question et même rejetés par les décideurs principaux et, ainsi, miner tout le processus.

3.4 Normes de sécurité

3.4.1 Avantages

Les normes de sécurité possèdent des vertus remarquables telles la facilité d'application et l'uniformité des résultats dans des circonstances comparables. Ces avantages sont le fruit de leur inhérente simplicité comme mécanisme de gestion des risques. En général, le spécialiste de la sécurité définit simplement les biens menacés en plus, peut-être, de décrire brièvement l'environnement opérationnel connexe. Les normes pertinentes proposent ensuite une liste de mesures de protection recommandées qui incluent, le cas échéant, quelques options ou compromis. Puisque les choix se limitent généralement à un éventail donné de biens d'une configuration particulière, les solutions ultimes sont habituellement uniformes pour l'ensemble des plates-formes et, ainsi, favorisent l'interopérabilité et l'intégration des systèmes. Bien que ces normes exigent une recherche fondamentale sous-jacente considérable, leur application fondée sur une approche de liste de contrôle exige beaucoup moins de temps et d'expertise qu'une EMR officielle. Pour autant que les normes sont raisonnablement à jour, les mesures de

protection recommandées demeurent toujours efficaces et offrent une assurance très élevée de réduction des risques significatifs puisque la majorité d'entre elles présument de l'existence d'un environnement de menace élevée et visent à contrer les pires des scénarios.

3.4.2 Inconvénients

Dans la pratique, les normes de sécurité présentent deux faiblesses majeures. Premièrement, leur processus de développement est souvent lourd : recherche et consultation approfondies, suivies d'un processus de vote prolongé, de révisions supplémentaires et, enfin, d'un processus officiel d'approbation et de promulgation. De tels travaux prolongés sont presque inévitables pour s'assurer que les normes proposées sont évaluées en détail et généralement acceptées, mais la longue période de gestation produit également de sérieux effets secondaires. Les nouvelles technologies émergent beaucoup plus rapidement que les normes de sécurité qui les concernent et les gestionnaires de projet, les concepteurs de systèmes et les spécialistes de la sécurité ont souvent des choix difficiles à faire sans aucune directive ni orientation. Là où des normes existent, leur utilité est souvent compromise pour les mêmes raisons. En effet, un trop grand nombre d'entre elles sont mises à jour peu fréquemment en raison des efforts laborieux que cela exige. Le manque de souplesse est la seconde faiblesse sérieuse de plusieurs normes. Aux fins de simplicité, la plupart des variables de risque sont intégrées à un petit nombre de solutions distinctes. Dans le domaine de la cryptographie, par exemple, une seule norme s'applique à tous les documents classifiés, quel que soit leur niveau de sensibilité, dans presque tous les environnements de menace. Cela soulève la question suivante : si une norme cryptographique est conçue pour protéger le trafic le plus sensible lors de transmissions internationales, n'est-elle pas trop stricte pour les documents moins sensibles transmis dans les réseaux nationaux? Effectivement, les normes de sécurité imposent souvent des solutions excessives pour éliminer complètement les risques plutôt que de gérer le problème à un coût plus raisonnable, ou du moins abordable.

3.5 Évaluation officielle des menaces et des risques

3.5.1 Avantages

L'approche de gestion des risques que propose l'EMR officielle tend à traiter certaines des plus sérieuses faiblesses des normes de sécurité. Une fois qu'une méthodologie d'EMR a été choisie, elle peut être appliquée immédiatement à n'importe quelle technologie émergente. Pour autant que l'outil soit à la fois modulaire et extensible, l'analyse peut cibler un nombre restreint de problèmes et apporter des solutions ponctuelles à des préoccupations immédiates. Dans la plupart des cas, l'évaluation fournit une justification explicite et entièrement transparente des solutions recommandées, ce qui aide à vaincre la résistance aux dépenses inévitables. De plus, il est possible de minimiser le coût réel des mesures de protection puisque l'évaluation tient compte à la fois des menaces et des vulnérabilités ainsi que des valeurs des biens, ce qui permet d'éviter certaines des recommandations les plus extrêmes. Cette souplesse inhérente est l'un des avantages les plus significatifs de l'évaluation des menaces et des risques. Un autre avantage est la piste de vérification explicite qu'offre une documentation exhaustive des décisions de sécurité, plus particulièrement s'il devenait nécessaire de démontrer qu'il y a eu diligence raisonnable à la suite d'un incident grave.

3.5.2 Inconvénients

De nombreuses publications, tant des secteurs public que privé, décrivent de manière très détaillée différentes méthodologies d'évaluation des menaces et des risques; toutefois, un trop grand nombre de ces méthodologies ne parvient pas à former un processus complet. Par exemple, certains manuels offrent peu de directives et d'orientation sur des aspects fondamentaux tels l'évaluation des biens et les paramètres de menace, et omettent même de définir de manière acceptable ce qu'est une vulnérabilité. Les incohérences et les insuffisances inhérentes à plusieurs outils ont eu tendance à décourager certains professionnels de la sécurité qui, de manière générale, se sont détournés des EMR. D'autres ont appliqué des techniques déficientes sans comprendre leurs conséquences possibles et ont ainsi obtenu des résultats imprévus, voire contradictoires. À l'occasion, des recommandations disparates de méthodologies différentes ont eu une incidence négative sur l'interopérabilité tout en minant la crédibilité du processus. Les évaluations des menaces et des risques souffrent également d'une autre lacune importante. L'effort nécessaire à la collecte de suffisamment de données pour produire un rapport d'EMR complet peut être très déconcertant et extrêmement coûteux, plus particulièrement dans le cas de situations ou de scénarios complexes. L'absence de dépôt central d'information sur les menaces au gouvernement fédéral ne fait qu'accentuer une charge déjà astreignante. Des contraintes de temps empêchent donc souvent l'exécution de travaux de cette ampleur et les gestionnaires de projet se tournent fréquemment vers d'autres méthodes moins coûteuses pour obtenir des résultats plus rapidement afin de réduire au minimum l'incidence sur des calendriers stricts et occasionnellement irréalistes. Même si la *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)* s'efforce de remédier à ces lacunes, l'expertise nécessaire à la réalisation de projets d'EMR efficaces n'est pas toujours disponible.

4 Application

4.1 Généralités

Chaque approche de gestion des risques possède des attributs à la fois positifs et négatifs. Une fois reconnus ces avantages et inconvénients, certains pouvant être la cause de réelles vulnérabilités, il semble aller de soi que des options différentes sont mieux adaptées à des circonstances elles aussi différentes. Il faut donc tenir compte de certains des facteurs les plus importants lors de la sélection d'une méthodologie de gestion des risques, notamment :
(1) contraintes de coût et de temps, (2) complexité de l'installation ou du système, (3) durée du projet, (4) disponibilité de normes et de professionnels de la sécurité appropriés et, surtout, (5) environnement de risque actuel et prévu.

4.2 Évaluation non officielle des menaces et des risques

Une approche minimaliste de la gestion des risques est appropriée seulement dans certaines circonstances très particulières. On doit donc, inéluctablement, l'utiliser pour obtenir une décision immédiate lorsque de sérieuses contraintes de temps empêchent d'effectuer une analyse plus rigoureuse. En effet, pour répondre à des situations d'urgence, toute intervention observée est préférable à une absence de décision prolongée. Dans un environnement de risque minime, où les valeurs des biens, les menaces et les vulnérabilités sont très faibles, cette approche peut

être raisonnable, plus particulièrement lorsque les coûts sont sérieusement préoccupants et qu'aucun expert en sécurité approprié n'est disponible pour effectuer une évaluation plus éclairée. De plus, une EMR non officielle ou superficielle est fréquemment utile pour déterminer si les normes de sécurité de base sont suffisantes, ou si une EMR officielle est requise. Lorsque, pour des motifs d'urgence, l'on recourt à des évaluations non officielles pour des biens plus complexes exposés à un certain niveau de risque, celles-ci doivent être réexaminées dans les plus brefs délais et complétées par l'application d'une des techniques plus exhaustives.

4.3 Spécialistes compétents

Lorsque des spécialistes compétents appropriés sont facilement disponibles, on peut utiliser efficacement cette approche de gestion des risques dans plusieurs circonstances différentes en raison de sa souplesse. En l'absence de normes de sécurité pertinentes, des spécialistes expérimentés peuvent répondre à des besoins immédiats très rapidement en effectuant un examen ciblé des problèmes particuliers. Puisqu'il faut plus de temps pour évaluer des systèmes complexes, les avantages de cette approche sur les évaluations officielles des menaces et des risques tendent à diminuer. Compte tenu de la subjectivité de cette approche, elle peut mieux convenir à des installations d'un seul occupant ou à des systèmes discrets plutôt qu'à des installations partagées ou à des environnements inter-réseaux sauf, évidemment, si les mêmes ressources sont utilisées pour chaque module ou sous-composante. En dernière analyse, les considérations de coût sont un important déterminant, et le recours à du personnel résident compétent plutôt qu'à des consultants plus dispendieux peut être un facteur important. On peut atténuer considérablement cet inconvénient en confiant comme seule tâche à des consultants le soin d'examiner les faiblesses particulières du personnel interne. Enfin, dans un contexte litigieux, un rapport narratif bien écrit peut ne pas offrir la transparence nécessaire pour démontrer qu'il y a eu diligence raisonnable dans l'éventualité d'une infraction sérieuse à la sécurité. Le recours à des spécialistes du domaine compétents peut annuler ce risque; toutefois, l'application de techniques plus objectives peut être préférable pour obtenir une piste de vérification plus valable.

4.4 Normes de sécurité

Les normes de sécurité, lorsqu'elles sont disponibles, sont très utiles dans plusieurs situations. Par exemple, il est beaucoup plus simple et rapide d'appliquer des normes connues que d'effectuer un projet d'évaluation officielle des menaces et des risques, ou même de consulter des spécialistes compétents. Donc, ces normes sont généralement plus appropriées lorsque d'importantes contraintes de temps ou des calendriers rigides imposent une solution immédiate à des problèmes particuliers. Même si les normes en question exigent une suite de mesures de protection plus coûteuses, la rapidité de l'intervention peut justifier les coûts supplémentaires à court terme. On peut ensuite recourir à d'autres techniques ultérieurement pour réviser les exigences de base et réduire les frais supplémentaires non justifiés. Là où il y a une rareté d'experts en sécurité, des employés moins qualifiés peuvent appliquer les normes avec plus de confiance. Dans un environnement réfractaire au risque, les normes de sécurité sont souvent préférables puisqu'elles offrent des solutions très sûres. À l'occasion, des accords internationaux ou des obligations contractuelles peuvent exiger des normes spécifiques dans

certaines conditions et, ainsi, ne laisser aucun choix au professionnel de la sécurité. Enfin, les normes de sécurité de base doivent être appliquées conformément à la PGS.

4.5 Évaluations officielles des menaces et des risques

Une évaluation abrégée des risques, qui vise seulement quelques menaces à l'égard d'un bien individuel, peut être effectuée presque aussi rapidement que n'importe quelle autre technique. Cette approche est particulièrement utile lorsqu'on l'utilise dans le cadre d'un examen de sécurité plus important où aucune norme n'a encore été définie pour les technologies plus récentes. Un projet d'EMR étroitement ciblé est également pratique dans le cas de menaces ou de vulnérabilités imprévues, ou pour évaluer des options moins coûteuses lorsque les normes approuvées ne conviennent pas ou que leur coût est exorbitant. Une évaluation plus détaillée d'un système ou d'une installation au complet nécessitera certainement beaucoup plus de temps et son coût sera beaucoup plus élevé. Ainsi, les EMR officielles sont fréquemment mieux adaptées à un environnement de projet lorsque le processus peut être planifié à des stades appropriés du plan de projet plan ou du cycle de développement de système. Les économies potentielles découlant d'une analyse plus détaillée qui permet d'adopter une suite de mesures de protection convenables justifieront souvent les heures, les efforts et les coûts supplémentaires.

4.6 Sommaire

Selon les circonstances, plus particulièrement lorsqu'il y a urgence et que l'exigence est complexe, n'importe laquelle des approches de gestion des risques peut convenir au développement de saines solutions de sécurité. Évidemment, certaines sont plus appropriées pour des scénarios à risque élevé alors que d'autres peuvent être mises en œuvre plus rapidement. Certaines approches sont mieux en mesure que d'autres de traiter les technologies émergentes, mais elles offrent toutes des avantages potentiels et méritent un examen attentif.

Le choix effectué par les spécialistes de la sécurité peut avoir de sérieuses incidences sur le résultat final d'un projet. Le recours à une approche minimaliste dans un environnement où les menaces sont élevées peut faire en sorte que des biens de valeurs continuent d'être exposés au risque. Le respect aveugle de normes désuètes est susceptible d'entraîner des dépenses inutiles ou, pire encore, d'être à l'origine d'importantes vulnérabilités. La rareté des spécialistes compétents fait en sorte que ceux-ci peuvent avoir leurs propres motifs cachés, ce qui peut créer des conflits d'intérêts, alors que des projets d'EMR complet peuvent être impossibles compte tenu d'aspects pratiques telles les valeurs des biens et les contraintes de temps et de coût. Pour obtenir des résultats qui répondent à des exigences opérationnelles réalistes, les gestionnaire de risques doivent se familiariser avec les différentes options et leurs forces et faiblesses inhérentes.

Dans le cas de systèmes plus simples ou de problèmes particuliers, l'alternative préférée peut être évidente, mais seulement intuitivement et en fonction des critères de sélection examinés précédemment. Toutefois, pour des systèmes plus complexes ou des programmes complets, le bon choix peut être moins évident. En fait, les différentes méthodes ne sont pas mutuellement exclusives et on peut utiliser une ou plusieurs techniques combinées pour obtenir des résultats ciblés plus précis. Par exemple, on peut appliquer des normes prouvées à un bien d'une installation ou à une composante d'un système, et recourir à une EMR officielle pour évaluer la

posture de sécurité des autres éléments ou services. Une EMR superficielle ou une approche minimaliste peut s'avérer suffisante pour certains aspects, par exemple où les valeurs des biens ou les menaces sont faibles tel qu'il est expliqué à la section 4.2, libérant de ce fait les rares ressources de sécurité qui pourront se concentrer sur les autres fonctions plus importantes. En résumé, la réelle puissance de ces différentes méthodologies tient à la synergie qu'elles favorisent lorsque, à la recherche de solutions rentables, l'on choisit méticuleusement des approches complémentaires pour atteindre un équilibre entre les besoins opérationnels et les préoccupations de sécurité.

5 Conclusion

Pour protéger les biens sensibles, la Politique du gouvernement sur la sécurité prescrit une gamme de mesure de protection fondées sur des normes de sécurité de base et la gestion continue des risques découlant d'une évaluation des menaces et des risques. Néanmoins, d'autres options, tel le recours à des spécialistes compétents, méritent également d'être utilisées dans certaines circonstances.

Des techniques plus objectives, plus particulièrement l'application de normes de sécurité et de projets officiels d'EMR, sont généralement préférables pour obtenir des résultats uniformes. De telles solutions communes sont particulièrement importantes pour promouvoir l'interopérabilité dans les environnements hautement réseautés d'aujourd'hui. Par contre, des techniques plus subjectives ont un réel mérite en l'absence de normes pertinentes, ou lorsque des contraintes de temps et de coût empêchent la tenue d'un EMR exhaustive.

Compte tenu des obligations plus importantes du gouvernement fédéral, la politique favorise à juste titre l'utilisation de normes de sécurité et d'EMR officielles; toutefois, à l'occasion, d'autres options sont nécessaires pour assurer plus de souplesse et de rentabilité, plus particulièrement lorsqu'elles sont appliquées collectivement pour répondre aux besoins immédiats d'une situation particulière. Pour s'assurer de faire un choix éclairé, les responsables de la sécurité et les gestionnaires de projet doivent comprendre les différentes méthodes, leurs forces et leurs faiblesses, ainsi que les circonstances où on doit les utiliser.

Appendice A-3 - Composition de l'équipe d'EMR

Ressources ministérielles		
Poste/Service		**Principales contributions**
Équipe de base	• Gestionnaire de programme • Autorité opérationnelle	• identification des biens (non techniques) • évaluation des biens/exigences opérationnelles
	• Administrateurs de système • Gestionnaires des installations	• identification des biens (techniques) • évaluation des vulnérabilités • mesures de protection (techniques) existantes • évaluation des menaces
	• Gestionnaire de projet • Architecte de la sécurité (système)	• identification des biens (techniques) • mesures de protection (techniques) existantes ou proposées • vulnérabilités techniques • recommandations (techniques)
	• Responsables de la sécurité o ASM o CTSI o CPCA	• évaluation des menaces • mesures de protection existantes ou proposées o ASM – programme global de sécurité o CTSI – sécurité des TI o CPCA – plans de continuité des activités/ ARO • conseils sur le processus d'EMR • fonction d'assurance de la qualité
Autres ressources internes	• Coordonnateurs de l'AIPRP	• considérations relatives à l'accès à l'information et à la protection des renseignements personnels/EFVP
	• Finances	• évaluation des biens • évaluation des menaces/pertes pour l'État
	• Ressources humaines	• questions se rapportant au personnel • menaces à l'endroit des employés
	• Vérification interne	• vérifications/examens ministériels • efficacité des mesures de protection par rapport aux vulnérabilités
	• Conseiller juridique	• obligations/responsabilités en vertu de la loi
	• Gestion du matériel	• identification et évaluation des biens
	• Santé et sécurité au travail	• certaines menaces (accidentelles) • mesures de protection s'y rapportant

Ressources externes		
Poste/Service		**Principales contributions**
Organismes conseils	• CST	• vulnérabilités techniques • menaces (techniques) • mesures de protection (techniques) • évaluations des menaces et des risques
	• SCRS	• évaluation des menaces
	• SPPCC	• évaluation des biens/infrastructures essentielles • évaluation des menaces • évaluation des vulnérabilités • plans de continuité des activités/ARO
	• TPSGC	• sécurité des marchés • identification des biens/infrastructures partagées
	• GRC	• évaluation des menaces • évaluation des vulnérabilités • mesures de protection physiques/opérationnelles
Autres organismes gouvernementaux	• MAECI	• évaluation des menaces : certaines menaces à l'étranger
	• Environnement Canada	• évaluation des menaces : certains risques naturels
	• Santé Canada	• évaluation des menaces : dangers pour la santé • évaluation des vulnérabilités
	• RHDSC	• évaluation des menaces : plusieurs menaces accidentelles • évaluation des vulnérabilités
Autres – Secteur public	• Service d'incendie	• évaluation des menaces
	• Service de police provincial/municipal	• évaluation des menaces
	• Services publics	• identification des biens (environnementaux) • évaluation des menaces • évaluation des vulnérabilités
Secteur privé	• Consultants	• en complément des ressources ministérielles • réalisation d'une EMR complète
	• Secteur de l'assurance	• évaluation des menaces • évaluation des vulnérabilités
	• Fournisseurs de produits	• évaluation des vulnérabilités • mesures de protection existantes ou proposées

Nota :

1. Cette liste n'est pas exhaustive. Les ministères devraient y ajouter tout autre poste/service pertinent, compte tenu de leur situation propre.
2. Les principales contributions de la troisième colonne se rapportent à des phases particulières d'un projet d'EMR au cours desquelles les organismes énumérés peuvent apporter une information utile.

Page intentionnellement laissée en blanc

Appendice A-4 - Recours à des consultants en EMR

1 Introduction

Lorsqu'il s'agit de constituer une équipe chargée d'effectuer une EMR, le recours à des consultants du secteur privé pour appuyer les ressources du ministère peut s'avérer très utile. Grâce à une planification sérieuse et à une gestion judicieuse, les avantages potentiels de l'emploi de consultants peuvent l'emporter de beaucoup sur les inconvénients possibles. Par ailleurs, une convention nationale cadre d'approvisionnement, établie par TPSGC, a simplifié le processus de passation de marchés pour les services de professionnels de la sécurité des TI notamment.

2 Avantages possibles

Le recours à des consultants peut offrir une marge de manœuvre appréciable dans le cadre d'un projet d'EMR. Par exemple, des entrepreneurs ayant les compétences voulues sont souvent immédiatement disponibles, si bien qu'ils peuvent être embauchés assez rapidement pour respecter des délais serrés, surtout lorsque les ressources du ministère sont déjà mises à rude épreuve.

Comme la plupart des fonctionnaires ont plusieurs responsabilités différentes, souvent assorties de priorités contradictoires, il peut être difficile pour eux de se concentrer pleinement sur une seule évaluation. Par conséquent, pour obtenir des résultats mieux ciblés, on peut confier à un consultant ou plus la tâche d'effectuer une évaluation particulière ou une partie de celle-ci.

Dans bien des organisations, le budget salarial est beaucoup plus limité que l'enveloppe des dépenses de fonctionnement et d'entretien (F et E). Ainsi, il peut s'avérer plus facile de retenir les services d'un consultant que de créer de nouveaux postes d'analystes affectés à l'EMR.

Lorsqu'une évaluation fait appel à des compétences spécialisées, les ressources du ministère peuvent être rares et même, dans le cas de certaines nouvelles technologiques, inexistantes. Pour éviter d'importants coûts de formation et les retards connexes pour ce qui pourrait s'avérer être un besoin ponctuel, il peut être préférable de retenir les services d'un consultant compétent. Le recours à des experts reconnus ayant les connaissances et l'expérience voulues peut également ajouter foi aux conclusions et recommandations formulées dans un rapport d'EMR, ce qui contribue à justifier les dépenses supplémentaires consacrées aux mesures de protection essentielles et, par la suite, si des risques se concrétisent, à montrer que l'organisation a fait preuve de diligence raisonnable.

En tant qu'intervenants de l'extérieur, les consultants abordent souvent les problèmes d'un point de vue différent, ce qui ajoute une perspective nouvelle, et à titre de tiers indépendants, peuvent fournir une analyse plus impartiale.

En règle générale, on s'attend à ce que les consultants ne travaillent pas sur place, ce qui signifie qu'ils n'ont besoin ni de fournitures de bureaux ni de locaux du gouvernement. Il peut s'agir d'un avantage important lorsque les locaux sont déjà occupés à pleine capacité.

3 Problèmes possibles

Pour optimiser les avantages associés au recours aux services de consultants en EMR, il faut tenir compte de certains problèmes éventuels et les régler dès le départ.

Lorsque les marchés dépassent les limites prévues pour les commandes directes, le recours au processus d'appel d'offres peut entraîner des retards, ce qui risque de nuire à l'ordonnancement des travaux. Ce problème peut être aggravé vers la fin de l'exercice lorsque de nombreux ministères attribuent un certain nombre de contrats pour aider à réduire les excédents et équilibrer leurs budgets.

Dans certains cas, la demande de consultants compétents peut excéder l'offre, de sorte qu'il peut être difficile d'obtenir une aide à plein temps, surtout à court préavis.

Alors que de nombreux entrepreneurs connaissent bien les différentes méthodes d'EMR et les technologies de l'information actuelles, ils sont moins susceptibles d'avoir des connaissances détaillées des programmes et des services ministériels qui font l'objet d'un projet d'EMR. Selon la complexité des biens visés et de l'environnement dans lequel ils se trouvent, il vaut peut-être mieux consacrer le temps prévu pour le transfert de ces connaissances aux consultants à la formation du personnel permanent sur le processus d'EMR.

La plupart des projets d'EMR comportent une certaine part d'informations sensibles, surtout en ce qui a trait aux menaces et aux vulnérabilités. Par conséquent, les consultants doivent posséder la cote de sécurité appropriée, alors qu'une attestation de sécurité d'installation est nécessaire pour leur entreprise. Cela ne pose pas de problème pour la plupart des entreprises établies, mais étant donné le taux de roulement élevé du personnel dans le secteur privé, le temps consacré aux évaluations de sécurité ou aux vérifications de la fiabilité peut entraîner des retards.

Malgré la contribution importante que des entrepreneurs peuvent apporter à une équipe d'EMR, le fait de trop compter sur leurs services peut constituer une entrave au perfectionnement de personnel compétent et créer ainsi une situation de dépendance permanente à l'égard de ressources externes plutôt qu'internes. À part les problèmes de moral qu'il risque d'entraîner, le recours à des consultants peut s'avérer peu économique parce que leurs services sont loin d'être donnés. En fait, les honoraires quotidiens de la plupart des entrepreneurs correspondent habituellement au double du salaire (avantages sociaux inclus) des employés possédant une expérience comparable.

4 Possibilités

Il existe bien des raisons d'avoir recours à des consultants pour des projets d'EMR, mais ce sont dans les circonstances suivantes que leurs services sont susceptibles de procurer les plus grands avantages :

- **Besoins urgents.** Lorsqu'il faut respecter l'échéancier d'un projet ou réagir à des incidents de sécurité dans des délais très courts, on peut avoir recours à un consultant en EMR ou plus pour venir en aide aux ressources du ministère et accélérer l'évaluation.
- **Expertise particulière.** Certains projets d'EMR peuvent parfois nécessiter l'accès à des compétences hautement spécialisées, et donc rares, pour l'évaluation de technologies particulièrement complexes et de menaces et vulnérabilités moins évidentes. À moins qu'une telle évaluation devienne une exigence courante, le recours à des consultants constitue probablement le meilleur moyen de répondre à des besoins ponctuels à court terme.
- **Crédibilité accrue.** Dans les situations délicates où un rapport d'EMR peut faire l'objet d'un examen minutieux du public en raison d'une compromission, le coût d'un spécialiste hautement qualifié peut être justifié pour ajouter foi aux recommandations finales et garantir leur qualité.
- **Périodes de pointe.** À titre de solution à court terme, on peut avoir recours à des consultants pour venir en aide au personnel pendant les périodes de pointe (voir la figure A4-1). Dans cet exemple, la demande prévue de services d'EMR occuperait à plein temps trois équivalents temps plein (ETP), mais l'accroissement de la demande à l'automne pourrait justifier le recours à un quatrième analyste. Au lieu de l'établissement d'un autre poste permanent, un marché d'une durée de 90 jours pourrait être conclu avec un consultant en EMR. Pour des projets de plus longue durée, par exemple six mois ou plus, le recours à des employés du ministère constitue en règle générale la solution la plus rentable.

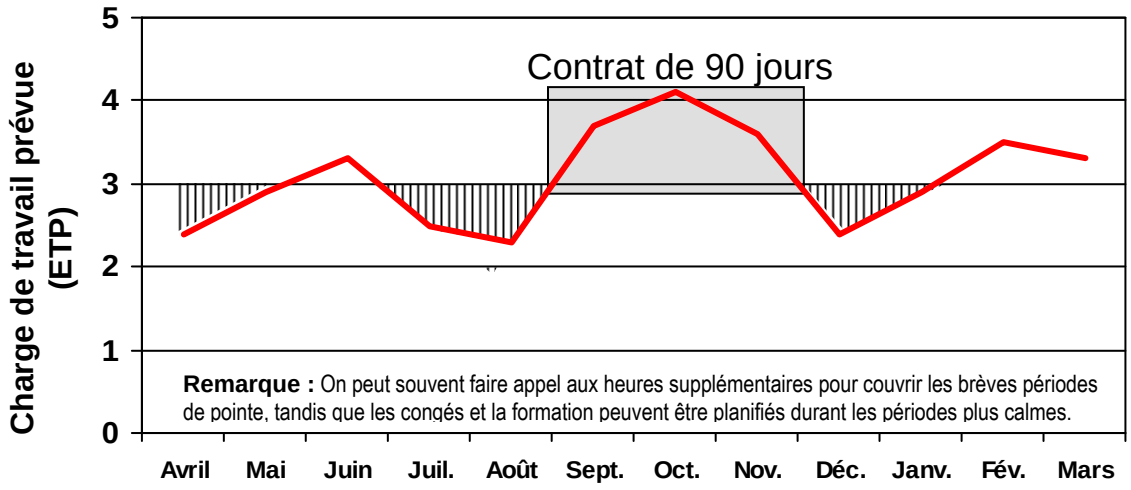

Figure A4-1 : Embauche de consultants pour accroître le personnel dédié aux EMR

- **Organisation dynamique.** Les entrepreneurs peuvent s'avérer particulièrement utiles aux organisations en transition. Par exemple, pendant des périodes de croissance rapide ou de réorganisation, des consultants en EMR peuvent assurer une stabilité précieuse et un mécanisme transitoire utile jusqu'à ce que les nouveaux postes soient finalement dotés et les membres du personnel entièrement formés. Dans le cas d'une réduction des effectifs, ils peuvent combler le vide laissé par les employés qui quittent, jusqu'à ce que la situation se stabilise.
- **Considérations budgétaires.** Lorsque des projets d'EMR font appel à des ressources supplémentaires, mais que l'enveloppe salariale est entièrement utilisée et qu'aucune réaffectation du personnel n'est possible, l'utilisation d'une partie du budget de F et E pour des marchés de services de consultants et de professionnels peut s'avérer la seule solution viable. En outre, vers la fin de l'exercice, il peut être rentable de retenir les services de consultants en EMR additionnels pour régler l'arriéré des évaluations en attente et éviter ce qui, autrement, pourrait se solder par un excédent budgétaire inacceptable.

5 Pratiques exemplaires

5.1 Généralités

Quelques pratiques exemplaires très simples relatives aux critères de sélection, à la passation des marchés et à la gestion subséquente du projet peuvent maximiser la contribution des consultants à une EMR.

5.2 Critères de sélection

Au moment de choisir un consultant en EMR, il faut tenir compte de plusieurs facteurs importants.

- **Connaissances.** Une bonne compréhension des pratiques de sécurité liées à l'évaluation est essentielle, surtout lorsqu'il est question de technologies nouvelles ou plus complexes. Une connaissance précise de la structure organisationnelle et des pratiques opérationnelles du ministère responsable du marché est d'une importance secondaire, mais constitue un atout souhaitable certain qui facilite l'évaluation.
- **Expérience.** Une expérience confirmée de la méthodologie d'EMR privilégiée est tout aussi importante pour éviter les retards et les malentendus.
- **Soutien.** Alors qu'un seul consultant peut offrir un excellent service, il est préférable en règle générale de compter sur le soutien d'une société de consultants, ce qui permet d'avoir accès à une plus vaste étendue de connaissances et de réduire au minimum les risques que le projet d'EMR soit retardé ou perturbé en cas d'accident ou de maladie du consultant principal.
- **Compétences.** La qualité des travaux antérieurs constitue normalement un bon indicateur du rendement futur. Il convient donc de tenter de déterminer dans quelle mesure la société de consultants a réussi à satisfaire d'autres clients.

- **Compatibilité.** La compatibilité du consultant avec la culture organisationnelle et les pratiques opérationnelles de la partie contractante est une question délicate mais potentiellement importante. Même l'entrepreneur le plus compétent peut échouer si son style personnel ou son comportement professionnel empêche une communication efficace et mine sa crédibilité.
- **Coût.** Pour assurer le meilleur rapport qualité-prix, il faut évaluer attentivement les honoraires des consultants en fonction des autres critères de sélection. Dans le cas d'un marché prescrit, il peut suffire de procéder à une comparaison subjective des coûts par rapport aux compétences professionnelles, mais pour un appel d'offres, il importe tout particulièrement de définir expressément à l'avance les facteurs de pondération, conformément à la section 5.3 ci-dessous, pour assurer la plus grande rentabilité possible.

5.3 Considérations contractuelles

Tous les marchés de services d'EMR doivent être conformes à la *Politique sur les marchés*, au *Guide des approvisionnements* et à la *Norme de sécurité et de gestion des marchés*. Plus précisément, les ministères devraient connaître les limites actuelles imposées dans le cas des marchés prescrits ou à fournisseur unique et des marchés sur appel d'offres traités à l'interne par rapport aux marchés conclus par l'intermédiaire de TPSGC. Il peut être préférable de séparer un grand projet d'EMR en plusieurs modules plus restreints, mais il faut éviter tout fractionnement ou toute perception de fractionnement d'un marché. Comme points importants à considérer, on retrouve notamment ce qui suit :

- **Limites contractuelles.** Les articles 16.10 et 16.11 de la *Politique sur les marchés*[1] renferment des directives explicites sur les marchés de services de conseil et de services professionnels. Les limites qui s'appliquent dans le cas des marchés de services concurrentiels et non concurrentiels sont énumérées à l'annexe 3 de l'appendice C de la politique, alors que l'annexe 5 fait état des limites encore plus strictes dans le cas des marchés de services conclus avec d'anciens fonctionnaires qui touchent une pension du gouvernement.
- **Énoncé des travaux.** Un énoncé des travaux clair est essentiel au succès de tout marché de services de consultants en EMR. L'énoncé des travaux doit définir à tout le moins l'objectif précis du projet d'EMR et présenter une description claire de toutes les tâches et de tous les produits livrables, accompagnée d'un exposé explicite des dates butoirs et des rapports hiérarchiques pour les rapports d'EMR provisoire et final, d'un énoncé précis des compétences que doit posséder l'entrepreneur, de la méthodologie à suivre, de toute exigence relative à la sécurité et de tous les documents de référence pertinents. L'appendice A-5 présente un exemple d'énoncé des travaux pour les services de consultants en EMR.
- **Dispositions standard.** Au moment de l'adjudication d'un marché, soit directement, soit par l'entremise de TPSGC, les ministères devraient inclure dans le contrat des dispositions standard concernant les droits de propriété intellectuelle à l'égard du rapport d'EMR et de tous les autres documents faisant partie du dossier de l'EMR. Les exigences en matière de sécurité, notamment les cotes de sécurité des consultants et si ceux-ci ne

[1] Voir le site Web du SCT : http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/Contracting/contractingpol_f.asp.

travailleront pas sur place, l'attestation de sécurité d'installation, constituent une autre considération importante. À cet égard, il convient normalement de dresser une Liste de vérification des exigences relatives à la sécurité (LVERS)2. Les responsabilités légales éventuelles peuvent également être une source de préoccupation pour le cas où des risques devaient se concrétiser malgré la mise en œuvre de toutes les mesures de protection recommandées dans le rapport d'EMR.

- **Rapport qualité-prix.** Pour les marchés concurrentiels, des critères d'évaluation pondérés devraient être expressément établis pour chaque facteur de sélection énoncé dans les documents d'invitation à soumissionner, tels que la Demande de proposition (DP), pour assurer l'optimisation des ressources. Autrement, un fournisseur moins compétent risquerait d'être retenu en présentant une offre artificiellement basse.

5.4 Gestion d'un marché d'EMR

Pour éviter les résultats imprévus, il ne faudrait pas s'attendre à ce que les consultants en EMR travaillent en vase clos ni même les autoriser à le faire. Des contacts réguliers avec le responsable technique dont le nom figure dans l'énoncé des travaux sont essentiels pour mener à bien un projet d'EMR. Plus précisément, le responsable technique doit s'acquitter des fonctions suivantes pendant toute la durée du marché :

- **fournir un soutien** pour s'assurer que l'entrepreneur a facilement accès aux employés et autres ressources du ministère, telles que des documents de référence et les biens matériels, afin qu'il puisse recueillir les données nécessaires à l'analyse le plus rapidement et le plus efficacement possible;
- **examiner les produits livrables** immédiatement pour éviter les retards indus;
- **offrir une rétroaction constructive** pour éviter les dérapages;
- **nommer du personnel à plein temps** chargé d'accompagner et d'aider l'entrepreneur dans la mesure du possible pour deux raisons : d'abord, pour optimiser les efforts du consultant en vue de produire une évaluation de qualité et, ensuite, pour profiter d'un certain transfert de connaissances qui aidera à former les employés du ministère;
- **examiner les résultats** d'une manière impartiale, non pas dans le but de critiquer le rendement de l'entrepreneur, mais de tirer des leçons pouvant améliorer les résultats des marchés de services de consultants en EMR subséquents.

6 Arrangement en matière d'approvisionnement en cyberprotection (AMAC)

Comme l'indique l'annexe A de la *Politique du gouvernement sur la sécurité* (PGS), le CST est l'autorité technique du gouvernement du Canada en matière de sécurité des technologies de l'information (TI). À ce titre, il a établi une convention nationale cadre d'approvisionnement sous les auspices de TPSGC pour faciliter la passation de marchés de services de gestion des risques pour la sécurité des TI, y compris les services de consultants en EMR. Les mécanismes

2 Le formulaire TBS/SCT 350-103 (2004/12) se trouve au site suivant : http://www.tbs-sct.gc.ca/tbsf-fsct/350-103_f.asp.

d'assurance de la qualité intégrés dans l'AMAC constituent un autre avantage important du programme[3].

[3] Voir le site Web du CST : http://www.cse-cst.gc.ca/services/cpsa/cpsa-program-f.html.

Page intentionnellement laissée en blanc

Appendice A-5 - Exemple d'énoncé des travaux pour les services de consultants en EMR

1 Objectif

Le présent énoncé des travaux décrit les travaux liés à l'exécution d'une évaluation des menaces et des risques (EMR) pour [*nom de l'installation/du système*]. [*Fournir une brève description de l'installation/du système dans le texte de l'énoncé des travaux et présenter en annexe les plans, les schémas et les autres renseignements pertinents.*] À tout le moins, l'EMR doit comprendre :

- un énoncé de la sensibilité qui identifie les biens pertinents et les classe selon le degré de préjudice qui pourrait vraisemblablement découler d'une compromission de leur confidentialité, de leur intégrité et de leur disponibilité;
- une description des menaces délibérées, des accidents et des risques naturels susceptibles de porter atteinte à ces biens, accompagnée d'une analyse de leur probabilité et de la gravité des conséquences;
- une évaluation des vulnérabilités actuelles, d'après un examen des mesures de sécurité existantes ou proposées et de leur efficacité;
- une analyse des risques résiduels pour chaque bien susceptible d'être exposé à des menaces précises;
- lorsque les risques résiduels éventuels dépassent le niveau [*Faible ou Moyen*], une liste des recommandations proposant des mesures de protection additionnelles pour atteindre un niveau de risque cible [*Faible ou Moyen*], ainsi qu'une évaluation de leur efficacité et de leur coût.

2 Tâches et produits livrables

2.1 Phase de préparation

2.1.1 Généralités

[*Les autorités ministérielles peuvent décider de mener la phase de préparation*[1] *à terme avant d'établir un énoncé des travaux pour les services de consultants en EMR, auquel cas cette section peut être omise. Toutefois, si les services d'un entrepreneur sont retenus pour la planification initiale, l'énoncé des travaux devrait comprendre une description générale de cette étape et des produits livrables.*] Une planification minutieuse est nécessaire avant d'amorcer une EMR afin de déterminer la portée de l'évaluation et les besoins en ressources et d'élaborer un plan de travail réaliste. Pour atteindre ces objectifs, l'entrepreneur doit collaborer étroitement avec le chargé de projet, le responsable technique, les responsables de la sécurité et les gestionnaires de l'installation ou du système. L'entrepreneur recevra tous les documents de référence énumérés à l'annexe A et toute autre information nécessaire à la réalisation de ce

1 Décrite à l'annexe A.

travail. Les activités de collecte de données peuvent comprendre des entrevues avec des employés à divers niveaux de l'organisation.

2.1.2 Produits livrables associés à la planification initiale

Le seul produit livrable pour la phase de préparation est un plan de travail de l'EMR complet[2] qui comprend :

- un énoncé clair de l'**objectif** de l'EMR;
- un énoncé de la **portée** accompagné d'une description de [*l'installation ou du système*] à l'étude, de sa mission et de son concept d'exploitation, ainsi que des limites de l'évaluation et de toute connexion avec d'autres [*installations ou systèmes*] ou de toute dépendance à l'égard de ceux-ci;
- les **limites** ou restrictions qui s'appliquent à l'EMR;
- le **niveau de risque cible** jugé acceptable par le gestionnaire responsable;
- une liste des employés qui participeront au processus d'EMR en tant que **membres de l'équipe** ou sources d'information;
- toutes les **dispositions logistiques** nécessaires, y compris les besoins en matière de filtrage de sécurité et d'accès, les dispositions de voyage, le soutien administratif et les autres besoins en matière de ressources;
- une liste des **documents de référence** et des **produits livrables**;
- un **calendrier** détaillé **de l'EMR** qui fait état de toutes les principales activités, des ressources qui y seront affectées, des dates de début et de fin et, s'il y a lieu, des facteurs qui en dépendent.

2.2 Évaluation des menaces et des risques

2.2.1 Généralités

Une fois que le plan de travail de l'EMR est approuvé, à la fin de la phase de préparation, l'entrepreneur veille à la mise au point de quatre produits livrables pour donner suite aux quatre étapes du processus d'EMR énoncées dans la *Politique du gouvernement sur la sécurité* (PGS)[3] :

- **identifier les employés et les biens** à protéger dans un énoncé de sensibilité;
- identifier les **menaces pour les employés et les biens** au Canada et à l'étranger, et évaluer la probabilité qu'elles se concrétisent ainsi que leur incidence;
- évaluer les **risques** en fonction de la pertinence des **mesures de protection existantes** et des **vulnérabilités**;
- recommander toute **mesure de protection supplémentaire** qui réduira les risques à un niveau acceptable.

[2] Un exemple de plan de travail de l'EMR figure à l'appendice A-6.

[3] Décrites dans le Sommaire de gestion.

2.2.2 Phase d'identification et d'évaluation des biens[4]

Au cours de cette deuxième phase, l'entrepreneur identifie les employés, les biens et les services visés par l'évaluation, en dresse la liste et leur attribue une valeur associée aux paramètres de confidentialité, de disponibilité et d'intégrité, selon le cas, en fonction des préjudices qui pourraient raisonnablement découler d'une compromission. Les résultats de cette analyse sont présentés, sous forme de tableau, dans un énoncé de sensibilité (le seul produit livrable pour cette partie du projet d'EMR) bien annoté pour justifier les conclusions[5].

2.2.3 Phase d'évaluation des menaces[6]

Au cours de la troisième phase d'un projet d'EMR, l'entrepreneur fait état des menaces réelles et potentielles qui pourraient raisonnablement porter préjudice aux employés, aux biens ou aux services. Il obtient des informations pertinentes sur les menaces auprès des responsables de la sécurité du ministère et des principaux organismes responsables, notamment le SCRS, le CST et la GRC. Les principaux produits livrables de cette phase de l'EMR consistent en :

- une liste, sous forme de tableau, des menaces réelles et potentielles susceptibles de causer un préjudice aux employés ou de compromettre les biens et les services visés par l'évaluation[7];
- une évaluation de la probabilité qu'elles se concrétisent et de leur incidence[8].

2.2.4 Phase d'évaluation des risques[9]

Au cours de la quatrième phase d'un projet d'EMR, l'entrepreneur évalue les risques résiduels pour les employés, les biens et les services relevés au cours de la deuxième phase et découlant des menaces analysées pendant la troisième phase. Les deux produits livrables obligatoires sont l'évaluation des vulnérabilités à la suite d'une analyse des mesures de protection existantes ou proposées et de leur efficacité[10], et l'évaluation des risques qui énumère tous les risques résiduels pour les employés, les biens et les services visés par l'évaluation[11].

2.2.5 Phase des recommandations[12]

À partir des conclusions de l'évaluation des risques effectuée au cours de l'étape précédente, l'entrepreneur propose l'ajout, la modification ou l'abandon de mesures de protection pour atteindre un niveau acceptable de risque résiduel[13]. Le risque résiduel projeté, c'est-à-dire le risque qui reste après l'approbation et la mise en œuvre des recommandations, est défini de façon explicite, tout comme les coûts des changements recommandés[14].

---

4 Décrite à l'annexe B.

5 Un exemple d'énoncé de sensibilité ou de tableau d'évaluation des biens figure à l'appendice B-5.

6 Décrite à l'annexe C.

7 Un exemple de tableau d'évaluation des menaces figure à l'appendice C-4.

8 L'appendice C-3 dresse la liste des mesures de la probabilité que les menaces se concrétisent et de leur incidence ou gravité et présente les calculs connexes.

9 Décrite aux annexes D et E.

10 Un exemple de tableau d'évaluation des vulnérabilités figure à l'appendice D-4.

11 Un exemple de tableau d'évaluation des risques figure à l'appendice E-2.

12 Décrite à l'annexe F.

13 L'appendice F-3 présente de façon explicite les critères de sélection des mesures de protection, alors que la liste des mesures de protection à l'appui des recommandations figure à l'appendice F-2.

14 Un exemple de tableau des recommandations figure à l'appendice F-5.

3 Gestion de projet

3.1 Chargé de projet

Le chargé du projet d'EMR est [*nom, titre du poste et numéro de téléphone du coordonnateur général du projet d'EMR choisi conformément à la section 5.4.7 de l'annexe A*].

3.2 Responsables techniques

Les responsables techniques pour ce projet sont [*nom, titre du poste et numéro de téléphone des spécialistes désignés qui assureront un soutien technique, y compris les responsables de la sécurité, les gestionnaires des installations ou les administrateurs des systèmes, ainsi que d'autres membres de l'équipe chargée de l'EMR*].

3.3 Méthodologie d'EMR

L'entrepreneur utilisera la *Méthodologie harmonisée d'évaluation des menaces et des risques (EMR)* pour ce projet. [*Indiquer d'autres documents s'il y a lieu*.]

3.4 Compétences du personnel

L'entrepreneur doit assurer les services d'un effectif ayant une vaste expérience et une solide connaissance du processus d'EMR et de l'objet de l'évaluation, telles qu'elles ont été démontrées par l'achèvement avec succès d'au moins trois autres EMR antérieures portant sur des [*installations ou des systèmes*] similaires.

3.5 Exigences en matière de sécurité

Le présent énoncé des travaux est [*classifié au niveau (indiquer le niveau) ou catégorisé au niveau (indiquer le niveau)*]. Les travaux exécutés dans le cadre de ce marché seront [*indiquer la classification de sécurité*], et les produits livrables à présenter à l'achèvement des travaux et décrits en détail dans le présent document seront [*indiquer la classification de sécurité*]. Les analystes de l'entrepreneur doivent posséder une cote de sécurité valide au moins au niveau exigé pour les travaux et les produits livrables. [***Nota :*** *L'énoncé de sensibilité indique la valeur des employés, des biens et des services, alors que l'évaluation des vulnérabilités énumère les attributs d'un bien ou de l'environnement dans lequel il se trouve auxquels des menaces visant à causer des dommages pourraient porter atteinte. Ce sont là des considérations importantes lorsqu'il s'agit d'attribuer une classification de sécurité (classifié ou protégé) aux produits livrables associés à une EMR. Lorsqu'il est question, dans le cadre de l'EMR, d'informations exclusives d'un tiers, tel que le fournisseur d'un produit, l'entrepreneur devrait être tenu de signer une entente de confidentialité appropriée.*]

3.6 Calendrier

Comme il est indiqué à la section 2.1 [*si l'entrepreneur doit procéder à la planification initiale*], l'entrepreneur doit élaborer un plan de travail de l'EMR qui renferme un calendrier détaillé faisant état des jalons, des activités essentielles et des facteurs qui en dépendent, aux fins de l'achèvement des travaux au plus tard [*à la date précisée par l'autorité contractante*]. À la suite de l'adjudication du marché, l'entrepreneur doit mener le projet d'EMR à terme [*dans les délais indiqués dans le plan de travail*] et soumettre en cours de route aux responsables techniques et au chargé de projet des produits livrables intermédiaires conformément au plan de travail approuvé. [*Par souci de clarté, chaque produit livrable ainsi que les dates butoirs connexes doivent être énumérés dans un tableau ou, dans le cas d'un projet d'EMR très complexe, un graphique Gantt.*]

3.7 Approbation des produits livrables

Tous les produits livrables doivent être examinés pour en assurer la qualité et l'exhaustivité, puis approuvés par les responsables techniques désignés avant l'amorce de la phase suivante du projet. Le rapport final d'EMR doit être approuvé par le chargé de projet avant que l'on puisse mettre un point final au marché.

3.8 Rapports d'étape

L'entrepreneur doit fournir régulièrement [*habituellement toutes les semaines*] des rapports d'étape au responsable technique désigné. Les rapports d'étape peuvent être présentés de vive voix. [*Si des rapports écrits sont préférables, il faut en indiquer la présentation et le contenu souhaités.*]

3.9 Lieu de travail

Tous les travaux doivent être exécutés dans les locaux de l'entrepreneur, sauf pour ce qui est des entrevues avec le personnel du ministère, qui seront coordonnées avec le responsable technique désigné. [*Si le projet d'EMR vise des informations sensibles, il faut s'assurer que l'entrepreneur a une attestation de sécurité d'installation avec capacité de protection de documents au niveau approprié, tel qu'il est indiqué à la section 3.5 ci-dessus.*]

3.10 Renseignements exclusifs

Tous les renseignements et documents mis à la disposition de l'entrepreneur au cours de ce projet sont jugés de nature exclusive et doivent être remis dès l'achèvement de l'EMR.

3.11 Transfert

Dans les deux (2) jours ouvrables suivant l'achèvement du projet à la satisfaction du chargé de projet, l'entrepreneur doit soumettre, à la réunion de transfert organisée par les responsables techniques :

- une liste de tous les changements apportés aux produits livrables à la suite des commentaires des responsables techniques et du chargé de projet;
- tous les produits livrables finals en [*préciser le format et le nombre d'exemplaires*];
- tous les renseignements de nature exclusive et les documents fournis à l'entrepreneur pendant la durée du projet.

Annexe A à l'exemple de l'énoncé des travaux

Références :

Politique du gouvernement sur la sécurité, Secrétariat du Conseil du Trésor, février 2002. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_f.asp

Norme opérationnelle de sécurité – Identification des biens, Secrétariat du Conseil du Trésor, ébauche.

Norme opérationnelle de sécurité – Programme de planification de la continuité des activités, Secrétariat du Conseil du Trésor, mars 2004. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/ossbcp-nsopca_f.asp

Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information, Secrétariat du Conseil du Trésor, avril 2004. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_f.asp

Norme opérationnelle de sécurité – Gestion des risques pour la sécurité, Secrétariat du Conseil du Trésor, ébauche.

Méthodologie harmonisée d'évaluation des menaces et des risques (EMR), Centre de la sécurité des télécommunications et Gendarmerie royale du Canada, août 2007.

Politique sur la protection des renseignements personnels, Secrétariat du Conseil du Trésor, décembre 1993. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1_f.asp

Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée – Cadre de gestion des risques d'entrave à la vie privée, Secrétariat du Conseil du Trésor, août 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_f.asp

Politique d'évaluation des facteurs relatifs à la vie privée, Secrétariat du Conseil du Trésor, mai 2002. http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_f.asp

Politique sur la gestion des risques, Secrétariat du Conseil du Trésor, avril 1994. http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/riskmanagpol_f.asp

Guide de certification et d'accréditation des technologies de l'information (MG-4), Centre de la sécurité des télécommunications, janvier 1996. http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg4-f.html

[*Il se peut que les documents de référence susmentionnés ne soient pas tous nécessaires pour une EMR donnée. Il suffit d'indiquer les documents applicables. Il faut ajouter tout autre document propre à l'objet de l'EMR, tel que les plans d'activités, les documents de conception et les évaluations des menaces pertinentes.*]

Page intentionnellement laissée en blanc

Appendice A-6 - Exemple de plan de travail de l'EMR

1 Contexte

Identifier l'organisation et fournir des renseignements de base pour situer l'évaluation dans le contexte du ministère. Selon l'objet de l'EMR, ces renseignements peuvent comprendre :

- une brève description du secteur d'activité et du contexte opérationnel;
- tout niveau de prestation de services ou toute obligation lié à l'évaluation;
- la justification de la mise en place d'une installation ou d'un système de TI nouveau ou amélioré;
- la nature de toute préoccupation particulière en matière de sécurité à laquelle il faut donner suite.

2 But

Énoncer l'objectif de l'évaluation dans une seule phrase, par exemple :

- « La présente EMR vise à évaluer les risques associés aux améliorations qu'il est prévu d'apporter à [*nom de l'installation*] et à recommander des mesures de protection appropriées. »
- « La présente EMR vise à évaluer les risques associés à [*nom du nouveau système de TI*] et à recommander des mesures de protection appropriées à l'appui de la certification et de l'accréditation de ce système. »
- « La présente EMR vise à évaluer le besoin de mesures de protection qui vont au-delà des exigences en matière de sécurité de base de [*nom de l'installation ou du système de TI*]. »

3 Portée

Identifier le sujet de l'évaluation et fournir une description générale de l'installation ou du système de TI visé. Les cartes, les graphiques, les plans d'étage et les schémas de système peuvent être particulièrement utiles pour délimiter la portée de l'EMR. Des annexes peuvent être utilisées pour présenter des listes des éléments qui s'inscrivent dans la portée de l'EMR et de ceux qui ne sont pas visés par l'évaluation[1].

Pour réduire au minimum le double emploi et restreindre le plus possible la portée, des projets d'EMR distincts peuvent être réalisés pour différents secteurs d'activité au sein d'une installation ou les principaux composants et modules d'un système de TI, tel qu'il est proposé à la section 4.3 de l'annexe A. Bien que chaque élément puisse être examiné de façon distincte, tous les éléments reliés devraient être indiqués ainsi que la nature de leur interdépendance.

[1] Ces listes peuvent être tirées de la liste détaillée des biens figurant à l'appendice B-2.

On peut aussi se servir d'un diagramme comme celui à la figure A6-1 pour représenter visuellement la portée de l'EMR. Dans cet exemple particulier représentant une coupe transversale d'un immeuble à quatre étages logeant quatre activités de programme distinctes, chaque secteur d'activité pourrait faire l'objet d'une EMR distincte et une cinquième évaluation pourrait viser la sécurité de base de l'immeuble. Puis, dans l'énoncé de la portée de l'EMR touchant les ressources humaines, la relation avec les autres évaluations pourrait être illustrée en conséquence.

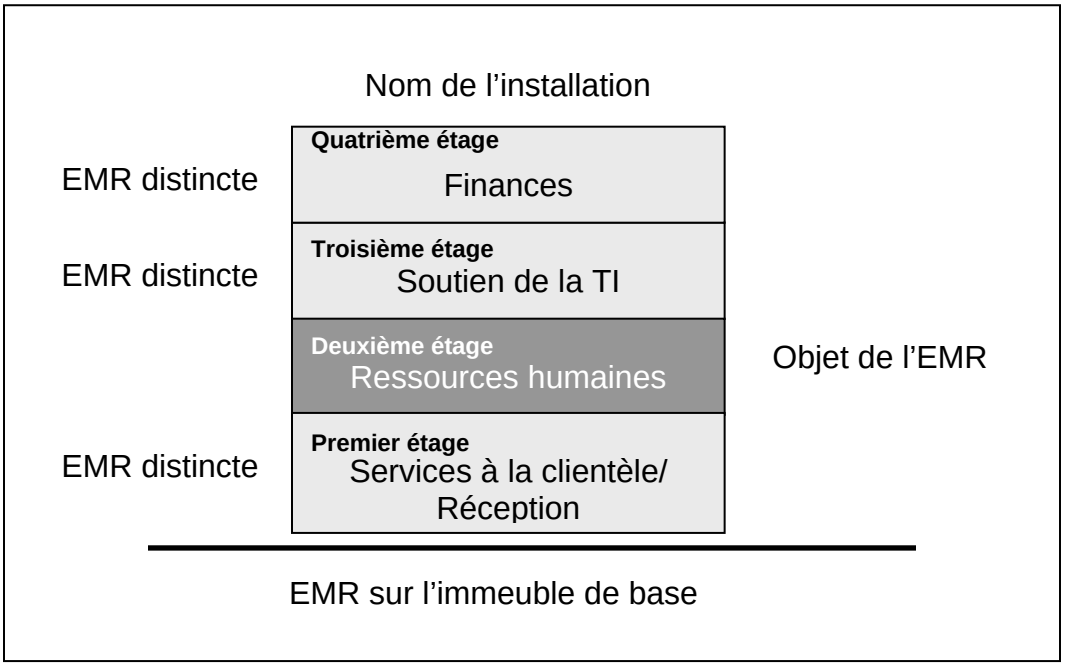

Figure A6-1 : Diagramme illustrant les projets d'EMR interreliés pour une seule installation

4 Limites

Identifier les limites ou restrictions qui s'appliquent à l'EMR, par exemple :

- les coûts ou les contraintes de temps susceptibles de nuire à la portée;
- l'inaccessibilité de biens aux fins d'examen;
- une absence de documentation susceptible de restreindre l'analyse;
- des exclusions délibérées de biens ou de menaces pour quelle que raison que ce soit, mais habituellement ceux qui n'ont qu'une faible incidence sur le risque global[2].

[2] Alors que la valeur des biens et les menaces sont normalement déterminées au cours des deux phases suivantes du processus d'EMR, tel qu'il est indiqué aux annexes B et C, certaines données sont évidentes dès le début et peuvent donc être éliminées de l'EMR. Par exemple, en règle générale, les fournitures de bureau non essentielles, surtout en petites quantités, sont omises de l'évaluation d'un contexte opérationnel normal.

5 Niveau de risque cible

Pour éviter la tendance à accroître la tolérance au risque lorsqu'il est recommandé, dans les conclusions d'une EMR, d'adopter des mesures de protection supplémentaires et potentiellement onéreuses, il faudrait que le niveau acceptable de risque résiduel soit énoncé à l'avance, avant d'entreprendre un projet d'EMR. Au départ, cela peut s'avérer difficile dans la pratique puisque les cadres supérieurs peuvent ne pas bien connaître le processus d'EMR et la nature du risque résiduel. Toutefois, une fois qu'une démonstration pratique de l'approche analytique a été faite, la réticence du début devrait normalement disparaître.

L'annexe E, intitulée Calcul des risques résiduels, examine plus à fond le risque résiduel et les paramètres connexes. La section 2 de l'annexe F, Phase des recommandations, traite des questions liées à l'acceptabilité mais en règle générale, un niveau de risque résiduel évalué comme étant faible ou moyen devrait être acceptable dans la plupart des cas. Tout niveau plus élevé est trop risqué, alors que les tentatives pour atteindre des niveaux de risque très faibles sont susceptibles d'être trop coûteuses et inutilement restrictives.

Ainsi, dans cette section du plan de travail de l'EMR, il suffit d'indiquer ce qui suit : « Le niveau de risque cible pour cette EMR est [*Faible ou Moyen*]. Dans la phase des recommandations, on proposera d'autres mesures de protection pour atteindre ce niveau maximal lorsque les risques résiduels sont évalués comme étant [*Moyen, Élevé et Très élevé/Élevé et Très élevé*]. »

6 Composition de l'équipe

Dresser la liste des membres de l'équipe de base et de leurs responsabilités ou contributions principales, ainsi que des autres ressources qui participeront à l'EMR. Une façon simple de présenter les informations requises consiste à utiliser un tableau comme celui qui suit.

Organisation	Membre(s) de l'équipe	Principales responsabilités
Secteur d'activité	Nom et poste	Identification et évaluation des biens
Bureau de projet	Nom et poste	Identification des biens Évaluation des vulnérabilités Recommandations
Agent de sécurité du ministère	Nom et poste	Évaluation des menaces Évaluation des vulnérabilités Recommandations
etc.		

Tableau A6-1 : Composition de l'équipe chargée de l'EMR

Le coordonnateur de l'équipe et le responsable de l'approbation ou de l'accréditation, dans le cas des évaluations de la sécurité matérielle et de la sécurité des TI respectivement, doivent être clairement identifiés.

7 Dispositions logistiques

Alors que les dispositions logistiques pour une EMR plus restreinte et ciblée peuvent être simples, elles peuvent s'avérer assez complexes dans le cas de grands projets de l'État vu le besoin de tenir compte de nombreux facteurs différents, dont :

- **les exigences en matière de filtrage de sécurité** visant à permettre aux membres de l'équipe d'avoir accès aux renseignements et aux installations associés à l'EMR, compte tenu du fait que les données relatives aux menaces et aux vulnérabilités en particulier sont souvent assez sensibles, comme il est indiqué à la section 5 de l'annexe G;
- **les exigences liées à l'accès** aux installations et aux données, tant matérielles que logiques, en fonction du besoin de connaître et non seulement de la cote de sécurité;
- **les dispositions de voyage**, des demandes officielles de visite étant présentées au besoin lorsque les installations sont réparties géographiquement;
- **le soutien administratif**, surtout l'aide de commis pour classer et récupérer la documentation, préparer des copies, consigner et distribuer la correspondance et libérer l'équipe d'analyse en accomplissant d'autres tâches courantes;
- les **autres besoins en ressources**, notamment les locaux, le matériel de bureau, la formation spécialisée et les fonds connexes nécessaires à l'achèvement du projet;
- s'il y a lieu, tout **énoncé des travaux** pour les services de consultants.

Un tableau simple devrait suffire à capter la plupart de ces renseignements, alors que les énoncés des travaux devraient être joints en annexe.

8 Documents de référence

Il est rarement possible d'énumérer dans un plan de travail de l'EMR toute la documentation utilisée, étant donné que du matériel de référence nouveau est susceptible de faire surface tout au long du processus d'analyse. Néanmoins, la plupart des documents de référence les plus importants devraient être identifiés à l'avance afin d'aider l'équipe chargée de l'EMR à partir du bon pied. Parmi ces documents, mentionnons les suivants :

- les politiques, les lois et les règlements fédéraux ayant trait à l'objet de l'évaluation;
- les politiques ministérielles et les plans d'activités;
- les protocoles d'entente visant le partage de renseignements et d'autres biens;
- les plans des installations et les dessins architecturaux;
- la documentation du projet, allant des exigences fonctionnelles aux dessins détaillés et tous les schémas ou plans de recolement connexes;
- toute vérification ou tout examen pertinent, ainsi que les rapports d'EMR antérieurs ou connexes;
- toute évaluation disponible des menaces et des vulnérabilités[3].

[3] Des listes plus complètes de documents de référence potentiels sont présentées aux appendices B-1 pour les biens, C-1 pour les menaces, D-1 pour les vulnérabilités et F-1 pour les mesures de protection.

Pour éviter que le plan de travail soit trop long, il y a lieu de regrouper dans une annexe la liste de tous les documents de référence.

9 Produits livrables

Dans tous les cas, le plus important produit livrable est le rapport final d'EMR qui fait état des risques résiduels et, au besoin, recommande des mesures de protection additionnelles pour atteindre des niveaux de risque acceptables. La présentation et le contenu général de ce rapport devraient être précisés dans le plan de travail. Des gabarits et un exemple de rapport d'EMR sont fournis aux appendices F-6 et F-7 respectivement.

D'autres documents peuvent être nécessaires dans le contexte d'un projet. Par exemple, une évaluation préliminaire de haut niveau peut tenir compte des exigences fonctionnelles pendant que d'autres améliorations sont apportées à différentes étapes du projet ou du cycle d'élaboration du système au fur et à mesure que le projet avance. À l'appendice A-1, on examine l'évolution d'une EMR tout au long du cycle d'élaboration d'un système général. Pour les projets d'EMR particulièrement complexes, des rapports d'étape sont souvent à conseiller pour s'assurer que les activités se déroulent comme prévu et pour repérer les obstacles éventuels le plus rapidement possible. Dans certains cas, les comptes rendus présentés de vive voix peuvent être acceptables, mais les rapports écrits sont généralement préférables pour assurer une documentation permanente.

10 Calendrier de l'EMR

Il est particulièrement important d'établir un calendrier réaliste pour l'EMR afin d'assurer une répartition plus efficiente des ressources et la gestion des attentes tout au long du processus. En règle générale, toutes les principales activités accompagnées des dates proposées de début et de fin, les ressources affectées à chaque tâche et, s'il y lieu, les liens entre les étapes devraient être énumérés. Alors qu'un tableau simple comme le tableau A6-2 qui suit peut suffire pour les rapports d'EMR plus courts, les évaluations plus complexes nécessiteront des mécanismes de planification et de suivi beaucoup plus évolués, tels que des graphiques Gantt ou PERT[4], ainsi que des outils automatisés pour leur génération et leur analyse, comme Microsoft ® Project[MC].

[4] *Méthode de programmation optimale*.

Série	Activité	Ressources affectées	Date de début	Date d'achèvement	Liens
1.	Identifier les biens				
2.	Attribuer des valeurs aux biens				Terminer n^{o} 1
3.	Identifier les menaces				
4.	Évaluer la probabilité/l'ampleur				Terminer n^{o} 3
5.	Évaluer les vulnérabilités				Terminer n^{o} 1
6.	Déterminer les risques résiduels				Terminer n^{os} 1 à 5
7.	Recommander des mesures de protection supplémentaires				Terminer n^{o} 6
8.	Présenter l'EMR final				Terminer n^{o} 7

Tableau A6-2 : Liste simple des activités de l'EMR

11 Approbation

Il est fortement recommandé de faire approuver officiellement le plan de travail de l'EMR par le gestionnaire responsable de la prestation des programmes ou des services qui sera appelé, au bout du compte, à accepter ou à rejeter les risques résiduels, afin de s'assurer qu'il comprend bien le processus d'EMR et les décisions qu'il devra prendre pour donner suite aux recommandations finales.

Approuvé.

Nom
Poste

Annexe B - Phase d'identification et d'évaluation des biens

1 Introduction

1.1 Généralités

Une fois le mandat d'un projet d'EMR établi, la portée de l'évaluation déterminée, l'équipe constituée et le plan de travail approuvé, l'analyse en tant que telle peut commencer avec la deuxième phase, la phase d'identification et d'évaluation des biens, qui comprend trois processus successifs et un résultat important, soit :

- **Identification des biens** – dresser la liste de tous les biens qui sont inclus dans la portée de l'évaluation à un niveau approprié de détail.
- **Évaluation des préjudices** – déterminer le préjudice qui pourrait vraisemblablement résulter d'une atteinte à la confidentialité, à la disponibilité ou à l'intégrité de chaque bien.
- **Évaluation des biens** – attribuer une valeur à chaque bien sur les plans de la confidentialité, de la disponibilité et de l'intégrité, selon le cas, en se fondant sur des critères de préjudice courants.
- **Tableau priorisé des biens** – rédiger l'énoncé de sensibilité, une liste exhaustive des biens, qui peuvent être classés par ordre décroissant de valeur.

1.2 But

Le but de cette annexe est de décrire les trois processus et le résultat unique de la phase d'identification et d'évaluation des biens d'un projet d'EMR.

1.3 Respect de la politique

Conformément à la section 10.6 de la PGS, Identification des biens, les ministères doivent identifier et catégoriser les biens dont la compromission risquerait vraisemblablement de porter préjudice à l'intérêt national ou à des intérêts privés ou non liés à l'intérêt national. Conformément à la section 10.7, Gestion des risques pour la sécurité, ils doivent identifier les employés et les biens à protéger. Ces exigences de la politique sont développées dans deux normes opérationnelles de sécurité, sur l'identification des biens et la gestion des risques pour la sécurité, respectivement. La phase d'identification et d'évaluation des biens d'un projet d'EMR prend ces exigences de la politique et les normes à l'appui comme point de départ et les pousse plus loin.

2 Identification des biens

2.1 Définition du terme « biens »

Tel qu'il est défini dans la PGS, le terme « biens » n'inclut ni les employés ni les services, qui doivent toutefois être protégés tous les deux conformément à l'objectif de la politique[1]. Par conséquent, pour déterminer les mesures de protection appropriées au-delà des exigences de base en matière de sécurité et de santé au travail, les employés et autres travailleurs, ainsi que les services qu'ils offrent, doivent être identifiés explicitement, à un niveau approprié de détail, s'ils sont inclus dans la portée d'un projet d'EMR.

> ***Biens** (assets)* – éléments d'actifs corporels ou incorporels du Gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale.
>
> *Politique du gouvernement sur la sécurité*, février 2002

2.2 Biens corporels

Les biens corporels sont généralement les plus faciles à identifier parce qu'ils comprennent les articles concrets, comme les installations, les véhicules, les meubles et fournitures de bureau, les œuvres d'art, les espèces et autres titres négociables, l'équipement des TI ainsi que les logiciels et micrologiciels connexes et les renseignements sous toutes leurs formes, sur support papier ou électronique. Le matériel de sécurité, qui va des systèmes d'alarme et contenants de sécurité aux logiciels antivirus et aux dispositifs cryptographiques, est un sous-ensemble spécial des biens corporels qui peuvent être exposés à des risques et qui, par conséquent, sont inclus dans la portée d'un projet d'EMR. Les ministères possèdent et exploitent de nombreux biens corporels, mais d'autres ne relèvent pas directement d'eux. Néanmoins, parce que la compromission de certains biens dans cet environnement pourrait avoir des répercussions négatives sur les opérations gouvernementales, il est souvent nécessaire d'étendre la portée d'une évaluation à d'autres choses, comme le réseau électrique ou la structure de l'immeuble dans lequel se trouvent des locaux loués, qui pourraient autrement être omises.

2.3 Biens incorporels

Les biens incorporels, comme le moral des employés et la confiance du public, sont dans une large mesure des questions d'attitude découlant de perceptions personnelles, tant individuelles que collectives. Ces perceptions de questions aussi variées que la qualité du service, le marquage des produits, les pratiques de gestion et les normes d'éthique sont souvent liées à la mission, à la vision et aux valeurs d'une organisation qui peuvent être mal définies et mal comprises. C'est

[1] La section 3 de la PGS, Objectif de la politique, se lit comme suit : « Soutenir l'intérêt national et les objectifs opérationnels du Gouvernement du Canada en assurant la sauvegarde des employés et des biens, ainsi que la prestation continue des services. »

pourquoi, les biens incorporels sont souvent plus difficiles à identifier et à catégoriser que leurs pendants plus concrets.

L'analyse des biens incorporels est aussi compliquée par le fait que relativement peu de menaces les touchent directement. Bien sûr, il existe quelques exceptions, comme la propagande subversive ou les rumeurs malveillantes, qui prennent explicitement pour cible le moral ou la confiance du public. Plus souvent qu'autrement, cependant, les préjudices causés aux biens incorporels résultent de la compromission de biens corporels ou d'employés et des services qu'ils offrent.

Malgré ces difficultés, il est absolument essentiel d'identifier les biens incorporels dans un projet d'EMR parce que les conséquences de leur compromission peuvent être plus graves que les préjudices correspondants pour d'autres biens. Par exemple, la divulgation sans autorisation de certains renseignements personnels concernant une seule personne peut causer un certain embarras ou un préjudice plus grave peut-être selon le niveau de sensibilité, mais la façon dont le public percevra la fuite peut causer plus de tort encore, minant la crédibilité de l'organisation et la confiance dont elle jouit en général.

Pour essayer de résoudre ce problème important, il faut identifier explicitement les relations entre les employés ou les biens corporels et les biens incorporels dérivés. Puis, étant donné que la plupart des mesures de protection protègent les employés ou les biens corporels directement et les biens incorporels indirectement seulement, harmoniser les valeurs attribuées aux premiers à celles des biens incorporels sous-jacents afin de leur assurer une protection adéquate.

2.4 Personnel

Bien que les employés et autres travailleurs ne soient pas considérés comme des biens dans le contexte de la PGS, ils ont besoin de protection pour au moins deux raisons importantes. Premièrement, les ministères sont astreints à des obligations très réelles aux termes du *Code canadien du travail*[2] et de diverses politiques du SCT, comme celle sur la *Sécurité et la santé au travail*[3] et la section 10.10 de la PGS, de protéger leurs employés contre tous les risques, des blessures accidentelles aux menaces de violence en milieu de travail. Deuxièmement, la disponibilité des employés qualifiés peut être une question lourde de conséquences selon la nature et l'importance des services qu'ils assurent. Afin de répondre à ces deux préoccupations au moyen de solutions de sécurité appropriées, il faut identifier les employés et autres travailleurs exposés à des risques pendant la deuxième phase d'un projet d'EMR.

2.5 Services

Les employés travaillent dans une large mesure avec des biens corporels pour offrir les services gouvernementaux, comme les soins de santé et le paiement des pensions. C'est pourquoi, du point de vue des ministères, protéger les employés et les biens selon les exigences de base en matière de sécurité et des projets d'EMR complémentaires pourrait suffire pour assurer une

[2] Disponible sur le site Web de Justice Canada : http://lois.justice.gc.ca/fr/showtdm/cs/L-2.
[3] Disponible sur le site Web du SCT : http://www.tbs-sct.gc.ca/pubs_pol/hrpubs/TBM_119/osh_f.asp.

prestation satisfaisante des services. Du point de vue des clients, cependant, les services eux-mêmes sont habituellement la considération la plus importante. C'est pourquoi, pour assurer une évaluation équilibrée à l'intérieur de la portée d'un projet d'EMR, il est important d'identifier tous les services rendus et d'établir des liens entre eux, les employés responsables et les biens pertinents.

2.6 Modèle d'identification des biens

La figure B-1 illustre les divers sujets de la phase d'identification et d'évaluation des biens d'un projet d'EMR, à savoir les employés et autres travailleurs qui utilisent des biens corporels pour offrir des services, dont la perception engendrera ou au moins touchera des biens incorporels, comme le moral des employés et la confiance du public.

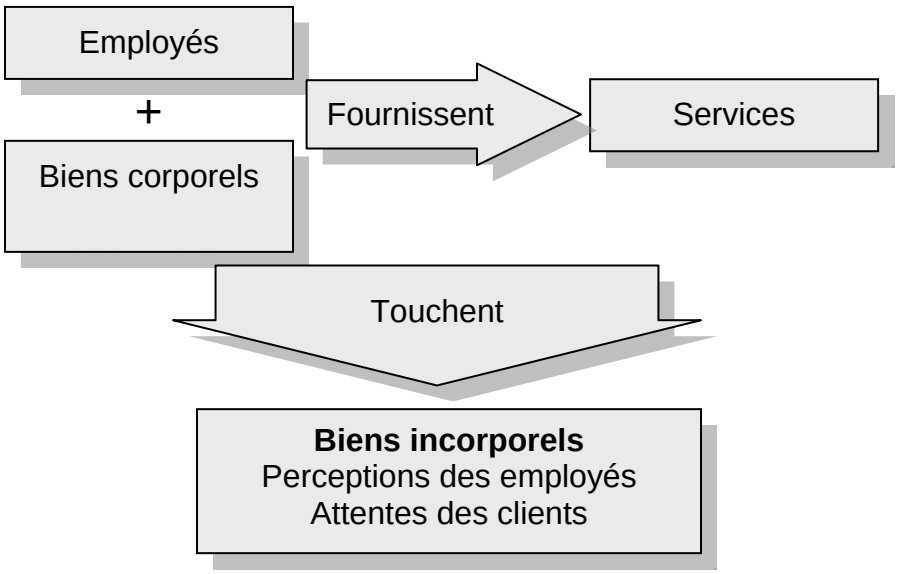

Figure B-1 : Modèle d'identification des biens

2.7 Sources de données sur les biens

Les données sur les biens et les valeurs qui y sont liées sont faciles à obtenir d'un grand nombre de sources différentes. Les gestionnaires de programmes et de projet sont souvent un point de départ logique pour recueillir des renseignements sur les employés, les biens et les services qu'ils offrent, mais de nombreux autres bureaux et représentants à l'intérieur d'un ministère peuvent apporter une contribution plus spécialisée, selon le sujet et la portée de l'évaluation. Certaines sources externes pourraient aussi être consultées, surtout en ce qui a trait aux biens environnementaux. L'appendice B-1 contient une liste de diverses sources de données éventuelles et des types de biens qu'elles peuvent identifier pour une équipe d'EMR.

2.8 Techniques de collecte de données

Les entrevues et les questionnaires peuvent être des méthodes utiles pour recueillir des données sur les biens, mais ils peuvent devenir coûteux et exigeants en main-d'œuvre pour les installations et systèmes plus grands. C'est pourquoi, il est souvent préférable de commencer par examiner les documents pertinents, comme les plans d'activités, les dessins architecturaux et les documents de conception. Puis, une fois qu'elle comprend mieux les biens en question, l'équipe d'EMR peut organiser des rencontres ciblées avec les responsables techniques et opérationnels afin d'obtenir plus de détails et de clarifier tout point litigieux. Cette façon de procéder est plus susceptible de réduire au minimum l'incidence sur les activités opérationnelles. Les visites et inspections sur place sont souvent utiles pour corroborer des constatations initiales. Dans certains cas, les interrogations des bases de données en regard des inventaires et des systèmes de gestion des biens peuvent fournir d'autres détails. Enfin, la *Méthodologie harmonisée d'EMR* comprend une liste exhaustive des biens à l'appendice B-2 qui pourra servir d'aide-mémoire pendant le processus d'identification des biens.

2.9 Liste des biens

2.9.1 Structure hiérarchique

La liste des biens qui se trouve à l'appendice B-2 est présentée sous forme de tableau hiérarchique allant des grandes classes et catégories de biens au plus haut niveau, aux groupes et sous-groupes de biens plus détaillés et même jusqu'à des éléments discrets pour une analyse de plus en plus granulaire. Cette structure est illustrée dans la figure B-2.

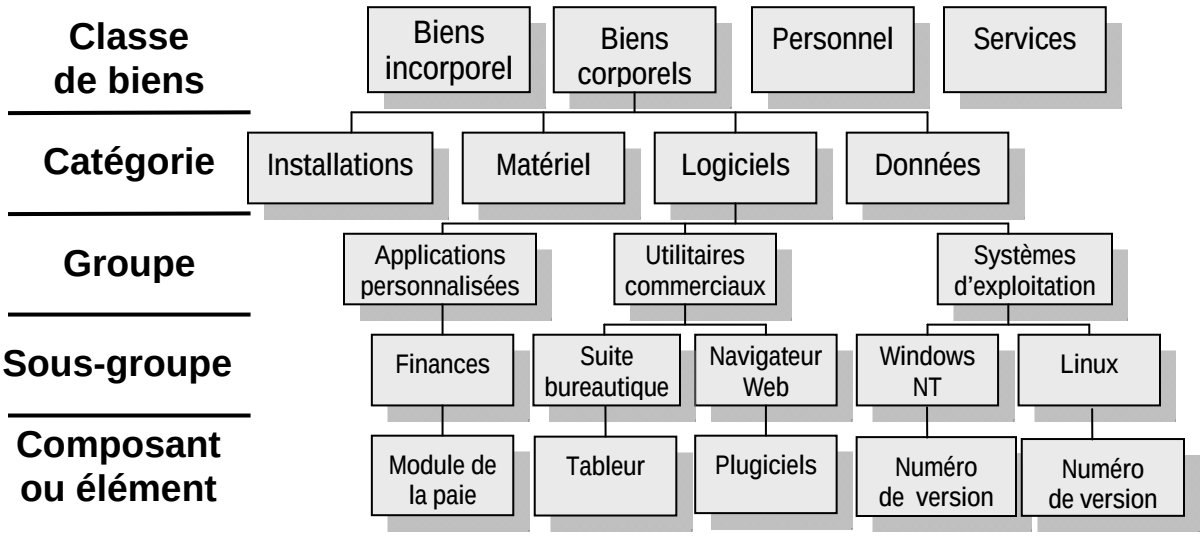

Figure B-2 : Exemple d'un segment de la structure hiérarchique de la liste des biens

2.9.2 Avantages possibles

La liste des biens hiérarchisée offre plusieurs avantages importants pendant la réalisation d'un projet d'EMR :

- **Cohérence.** L'utilisation de structures de données communes pour l'identification des biens facilite les communications à l'intérieur d'un projet d'EMR et entre les projets d'EMR pour parvenir à des résultats cohérents qui peuvent être reproduits par différents praticiens évaluant les mêmes biens ou des biens semblables. Elle favorise également l'interopérabilité et soutient le partage des biens entre les organisations.
- **Exhaustivité.** Les équipes d'EMR qui utilisent une liste exhaustive risquent moins d'omettre des biens importants.
- **Flexibilité et extensibilité.** Plus important encore, la structure hiérarchique de la liste des biens permet d'effectuer une analyse à des niveaux de détail différents, en fonction de la portée de l'évaluation et de l'environnement de risque exact. Essentiellement, les biens de moindre valeur assujettis à des menaces moins graves sont regroupés et évalués en plus gros groupes, tandis que ceux qui sont exposés à des risques plus élevés peuvent être examinés au niveau des sous-groupes ou même des éléments, pour plus de précision. De même, des branches entières de cette structure de type arborescente peuvent être ignorées complètement si une catégorie ou un groupe de biens précis n'est pas inclus dans la portée de l'évaluation. Les équipes d'EMR peuvent donc restreindre leurs efforts pour se concentrer sur ce qui est vraiment important, comme on peut le voir à la figure B-3.
- **Documentation à jour.** La liste des biens est facile à mettre à jour à mesure que de nouveaux produits ou services sont développés et déployés. De plus, étant donné les regroupements logiques de biens semblables, il est beaucoup plus simple de catégoriser les nouvelles technologies.

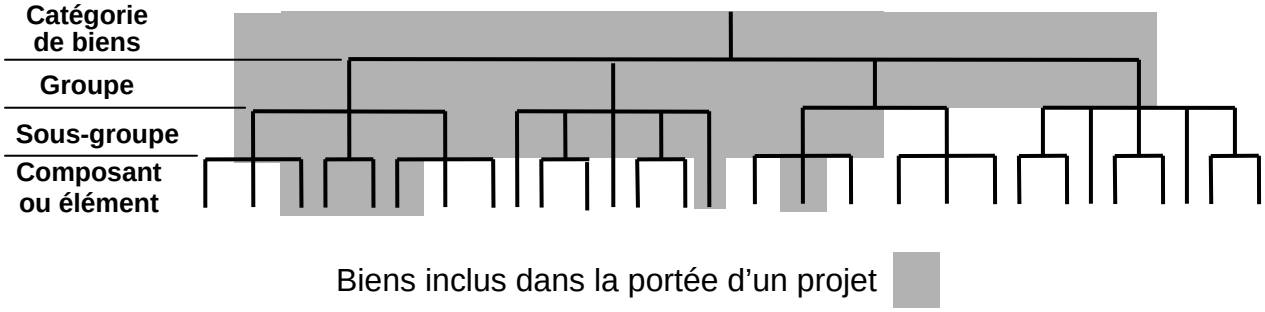

Figure B-3 : Sélection des biens inclus dans la portée d'un projet d'EMR

2.9.3 Mise en garde

Malgré ces nombreux avantages, la liste des biens doit être utilisée avec prudence. Elle n'est pas et ne pourra jamais être absolument complète parce que de nouveaux biens, surtout au niveau de détail des éléments, entrent en jeu régulièrement en raison, en partie, de l'évolution rapide des technologies et des nouvelles occasions opérationnelles. **C'est pourquoi, l'appendice B-2 devrait servir principalement d'aide-mémoire et de guide pour aider à organiser et à structurer la collecte et la compilation des données pertinentes sur les biens, plutôt que de liste de contrôle à suivre sans se poser de questions.**

3 Évaluation des préjudices

3.1 Exigences de la PGS

Conformément à la section 10.6 de la PGS, les ministères doivent catégoriser les renseignements et autres biens selon le degré de préjudice qui pourrait vraisemblablement résulter d'une compromission à leur confidentialité, leur disponibilité ou leur intégrité. Les biens dont la divulgation sans autorisation pourrait porter préjudice à l'intérêt national ou à d'autres intérêts doivent être identifiés comme classifiés ou protégés et être marqués selon le degré de préjudice potentiel. Sur les plans de la disponibilité et de l'intégrité, les biens doivent également être marqués en fonction du degré de préjudice. Le concept de valeur (reliée au patrimoine ou monétaire) est aussi introduit, sans système progressif de marquage en fonction du préjudice toutefois. Les niveaux précisés pour la confidentialité, la disponibilité et l'intégrité sont résumés dans le tableau B-1.

Les exigences de la PGS sont développées dans la *Norme opérationnelle de sécurité sur l'identification des biens* avec de nombreux exemples illustrant les divers degrés de préjudice résultant d'une atteinte à la confidentialité, à la disponibilité, à l'intégrité ou à la valeur. Inversement, les relations entre les degrés de préjudice Élevé, Moyen et Faible pour les biens protégés et Exceptionnellement grave, Grave et Préjudice pour les biens classifiés ne sont pas précisées.

Confidentialité		**Disponibilité**	**Intégrité**
Classifié (Intérêt national)	**Protégé (Autres intérêts)**		
Très secret Préjudice exceptionnellement grave	Protégé C : Élevé	Élevé	Élevé
Secret Préjudice grave	Protégé B : Moyen	Moyen	Moyen
Confidentiel Préjudice	Protégé A : Faible	Faible	Faible

Tableau B-1 : Catégorisation des biens selon les degrés de préjudice indiqués dans la PGS

3.2 Analyse comparative

3.2.1 Exigences analytiques

De toute évidence, les biens peuvent se voir attribuer une ou plusieurs valeurs selon l'incidence prévue (ou préjudice) d'une compromission. De plus, ces biens peuvent avoir la même valeur ou des valeurs différentes dans chacune des quatre ou cinq échelles (la confidentialité, selon qu'ils sont classifiés ou protégés, la disponibilité, l'intégrité et la valeur). Pour parvenir à faire une évaluation uniforme des biens et une analyse comparative de différents biens et valeurs de biens, et pour déterminer leur contribution relative au risque global, il faut énoncer clairement les relations entre chacune des quatre ou cinq échelles.

3.2.2 Harmonisation des valeurs des biens

La PGS et la *Norme opérationnelle de sécurité – Identification des biens* fournissent plusieurs indicateurs précieux donnant une idée de la façon dont les échelles d'évaluation des biens peuvent être harmonisées. Premièrement, les trois niveaux de préjudice définis pour la disponibilité, l'intégrité et la valeur, à savoir faible, moyen et élevé, semblent correspondre à Protégé A, B et C respectivement, comme on peut le voir à la section 10.6(a) de la PGS. Une correspondance semblable avec les valeurs de l'échelle Classifié est légèrement plus compliquée, mais la section 6.5.1.1 de la norme offre un cadre de référence, reconnaissant que la classification Diffusion restreinte est toujours utilisée par certains alliés et organisations internationales et la mettant sur le même pied que Protégé A. De même, la classification suivante, Confidentiel, peut être mise sur le même pied que Protégé B et le degré de préjudice moyen, et la suivante, Secret, sur le même pied que Protégé C et le préjudice élevé. Dans le haut de la gamme, la classification Très secret se retrouve seule, sans pendant dans l'échelle Protégé ou dans les échelles de la disponibilité, de l'intégrité et de la valeur, à moins que Protégé C et préjudice élevé soient l'équivalent de Secret (préjudice grave) et de Très secret (préjudice exceptionnellement grave). Cette formule a été rejetée, cependant, parce qu'elle pourrait estomper la distinction entre Secret et Très secret, si les deux étaient l'équivalent d'un degré de préjudice élevé sur l'échelle Protégé, et sur les échelles de la disponibilité et de l'intégrité.

3.2.3 Valeurs très élevées des biens

Dans des cas extrêmes, le préjudice résultant d'une atteinte à la disponibilité et à l'intégrité pourrait équivaloir celui causé par la divulgation sans autorisation d'un document Très secret. Par exemple, la modification sans autorisation des dossiers de patients dans un grand hôpital métropolitain pourrait provoquer de nombreuses pertes de vie, tout comme une panne de courant prolongée au milieu de l'hiver. Pour permettre une analyse plus granulaire à des fins de comparaison, la création d'un seuil explicite à l'intérieur de l'échelon élevé, au-delà duquel le préjudice sur les plans de la disponibilité, de l'intégrité et de la valeur deviendrait très élevé, l'équivalent de Très secret, semble donc être une solution plus appropriée.

3.2.4 Valeurs très faibles des biens

À l'autre bout de la gamme, de nombreux renseignements ont peu voire pas de valeur sur le plan de la confidentialité, de sorte qu'ils sont adéquatement catégorisés comme Non classifié. La section 6.2 de la norme *Identification des biens* reconnaît également que, dans certains cas, le préjudice résultant d'une atteinte à la disponibilité ou à l'intégrité peut être négligeable, justifiant de ce fait une valeur de bien très faible, comparable à Non classifié.

3.2.5 Niveaux de préjudices comparatifs

Suivant ce raisonnement, les exigences de la PGS et des normes de sécurité connexes, résumées au tableau B-1, peuvent être développées et étendues, comme on peut le voir dans le tableau B-2, pour permettre l'analyse comparative de différents biens, des valeurs de ces biens et de leur incidence relative sur les risques résiduels en fonction d'une échelle de cinq points allant de Très faible à Très élevé.

Niveaux de préjudice comparatifs	Type de compromission				
	Divulgation		Destruction Interruption Suppression	Modification	Destruction Suppression
	Confidentialité		Disponibilité	Intégrité	Valeur
	Classifié	Protégé			
Très élevé	Très secret		Très élevé	Très élevé	Très élevé
Élevé	Secret	Protégé C	Élevé	Élevé	Élevé
Moyen	Confidentiel	Protégé B	Moyen	Moyen	Moyen
Faible	(Diffusion restreinte)	Protégé A	Faible	Faible	Faible
Très faible	Non classifié		Négligeable ou très faible		

Tableau B-2 : Valeurs comparatives des biens

Nota : À titre de cas spécial, si la divulgation sans autorisation de renseignements protégés risquait de causer un préjudice très élevé, comme de nombreuses pertes de vies, les résultats auraient indubitablement une incidence sur l'intérêt national, justifiant de ce fait une classification Très secret.

3.3 Tableau des préjudices

3.3.1 Généralités

Bien que les conséquences d'une compromission puissent varier considérablement, selon la menace et les biens touchés, le résultat concret peut être ramené à un ou plusieurs de trois préjudices possibles, à savoir des dommages physiques ou psychologiques à des humains, ou une perte financière.

3.3.2 Dommage physique

L'incidence physique sur une personne peut aller d'un léger inconfort, à une blessure ou une maladie mineure, à une blessure ou une maladie grave et éventuellement à la perte de vie. Le nombre de personnes touchées par un seul événement constitue une deuxième dimension de l'évaluation. En effet, de nombreuses pertes de vie sont plus sérieuses que la perte éventuelle d'un seul être humain.

3.3.3 Dommage psychologique

L'incidence psychologique sur une personne peut aussi être mesurée sur une échelle graduée allant de l'inconvénient ou l'embarras mineur, à l'inquiétude sérieuse ou au stress, puis au traumatisme psychologique important. Là encore, la gravité du préjudice augmente avec le nombre de personnes touchées.

3.3.4 Pertes financières

Les pertes financières comprennent bon nombre de dépenses ou de coûts de renonciation associés à une menace causant un préjudice, comme la valeur de remplacement de l'équipement perdu ou volé, les coûts de reconstruction des installations endommagées ou de données corrompues, les pertes de revenus, les frais juridiques en cas de litige et les coûts de recrutement et de formation des employés de remplacement. Une fois ces diverses possibilités évaluées, le préjudice financier relatif peut être classé sur une simple échelle linéaire allant de moins de 1 000 $ à plus de 1 milliard de dollars.

3.3.5 Tableau comparatif des préjudices

Le tableau B-3 offre une version abrégée des échelles graduées de préjudices utilisées pour déterminer les valeurs des biens, qui vont de très faible à très élevée. Comme les mêmes mesures s'appliquent à tous les types de préjudices, qu'il s'agisse de la confidentialité, de la disponibilité ou de l'intégrité, le tableau des préjudices commun est un élément essentiel de la méthodologie harmonisée d'EMR qui permet d'effectuer une analyse comparative des différentes valeurs d'un seul bien ou de différents biens ayant différentes valeurs afin de déterminer lesquels sont associés aux risques les plus élevés. L'appendice B-4 contient une version élargie de ce tableau avec d'autres exemples et explications afin de faciliter le processus d'évaluation des biens.

Niveau de préjudice	Répercussions humaines		Répercussions financières
	Physiques	Psychologiques	
Très élevé	Pertes de vie massives	Traumatisme généralisé	> 1 G$
Élevé	Pertes de vie possibles	Stress/traumatisme grave	> 10 M$
Moyen	Blessures/maladies mineures	Méfiance/doutes du public	> 100 K$
Faible	Inconfort	Léger embarras	> 1 K$
Très faible	Négligeables	Négligeables	< 1 K$

Tableau B-3 : Tableau abrégé des préjudices et des valeurs des biens

3.3.6 Valeur maximale

Toute atteinte à la confidentialité, à la disponibilité et à l'intégrité d'un seul bien peut causer des préjudices à deux ou trois dimensions, c.-à-d. ayant à la fois des conséquences physiques et psychologiques pour des humains et entraînant peut-être aussi une perte financière. Lorsque les niveaux relatifs de ces différents préjudices résultant d'une seule menace touchant la valeur d'un seul bien (confidentialité, disponibilité ou intégrité) diffèrent, le niveau le plus élevé doit être attribué comme valeur ultime du bien. Par exemple, la divulgation sans autorisation d'un seul dossier du personnel, une atteinte à la confidentialité, peut ne pas causer de préjudice physique au sujet, de sorte que le niveau de préjudice physique connexe serait coté très faible. Si la perte était susceptible d'entraîner une peine de 5 000 $, cependant, le niveau du préjudice financier serait coté faible. Par contre, l'incidence psychologique sur la personne touchée par la compromission et sur d'autres personnes associées à l'organisation pourrait être beaucoup plus grave, amenant le public à se méfier et à avoir des doutes. Par conséquent, les renseignements en question se verraient attribuer une valeur de confidentialité moyenne (Protégé B) en raison du

préjudice psychologique parce que, dans ce cas, il s'agit de la conséquence la plus grave de l'atteinte à la confidentialité.

4 Évaluation des biens

4.1 Considérations générales

Tous les biens inclus dans la portée d'un projet d'EMR doivent se voir attribuer une ou plusieurs valeurs selon le degré de préjudice qui pourrait vraisemblablement résulter d'une atteinte à leur confidentialité (divulgation sans autorisation), à leur disponibilité (destruction, interruption, suppression ou utilisation sans autorisation) ou à leur intégrité (modification sans autorisation). Le niveau concret choisi dans le tableau élargi des préjudices de l'appendice B-4 devrait correspondre au pire des scénarios, à l'incidence maximale si le bien était totalement compromis. Dans la plupart des cas, les dommages réels et le risque connexe seront beaucoup moindres pour trois raisons :

- premièrement, les incidents sont rarement tellement extraordinaires qu'ils causent une compromission totale, parce que les agents de menace délibérés en sont souvent incapables et que l'ampleur de la plupart des accidents et catastrophes naturelles n'est pas absolue;
- deuxièmement, le risque ou la probabilité que la plupart des menaces surviennent n'est pas de 100 %;
- troisièmement, les mesures de protection existantes ont tendance à atténuer les effets de nombreuses vulnérabilités, de sorte que l'exposition même à des menaces graves peut être réduite considérablement.

Étant donné ces facteurs modérateurs, la plupart des risques sont moindres que la valeur réelle attribuée au bien. Cependant, plus les menaces sont proches du pire des scénarios et plus les vulnérabilités deviennent absolues, plus le risque résultant se rapproche de la valeur attribuée au bien, comme l'illustre la figure B-4.

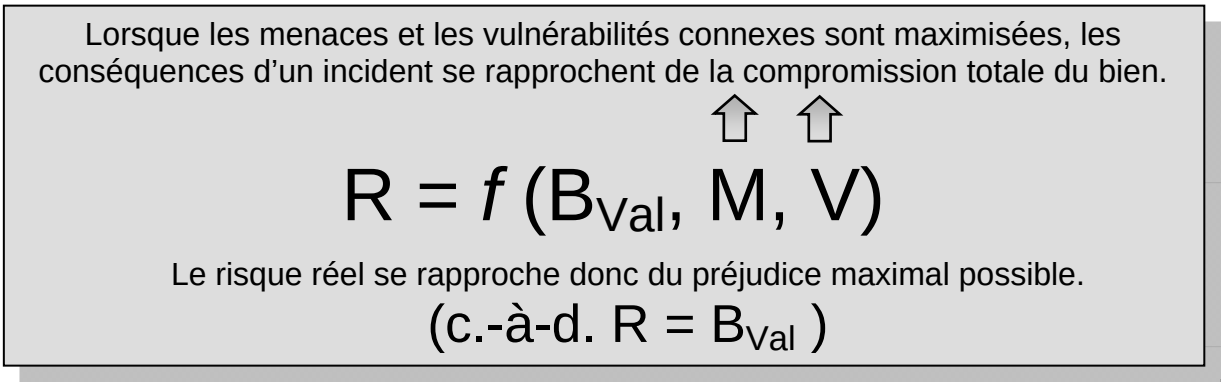

Figure B-4 : Valeurs des biens fondées sur une compromission totale

4.2 Application pratique

4.2.1. Généralités

Tous les biens doivent avoir au moins une valeur (disponibilité), mais très peu, exception faite des données ou des renseignements, en auront trois ou quatre (confidentialité, disponibilité, intégrité et valeur). Certaines des considérations pratiques qui suivent détermineront lesquelles parmi ces trois ou quatre valeurs s'appliquent à différents biens dans différentes circonstances.

4.2.2 Confidentialité

> ***Confidentialité*** (*confidentiality*) – caractéristique selon laquelle les renseignements ne doivent pas être divulgués à des personnes non autorisées, cela pouvant porter préjudice à l'intérêt national ou à d'autres intérêts, comme l'indiquent des dispositions précises de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*.
>
> *Politique du gouvernement sur la sécurité*, février 2002

La valeur de la confidentialité, c.-à-d. le préjudice qui pourrait vraisemblablement résulter d'une divulgation sans autorisation, s'applique certainement aux **renseignements**, qui peuvent tous être catégorisés et se voir attribuer des valeurs allant de très faible (Non classifié) à très élevée (Très secret). Certains **biens matériels** peuvent aussi nécessiter une protection pour des raisons de confidentialité. Par exemple, l'accès sans autorisation à certain matériel militaire pourrait révéler des capacités opérationnelles; l'analyse d'autres produits pourrait permettre de découvrir des secrets commerciaux, en recourant aux techniques de rétroingénierie au besoin; de même du matériel de sécurité informatique pourrait être étudié par des adversaires éventuels désireux de découvrir des vulnérabilités exploitables. Dans chaque cas, des préjudices perceptibles pourraient résulter de la divulgation sans autorisation des caractéristiques des biens, de sorte que le matériel concerné doit être identifié et se voir attribuer les valeurs de confidentialité appropriées. Bien que les renseignements sur les **employés** et autres **travailleurs** puissent être sensibles à une divulgation sans autorisation, et que les gens doivent posséder des cotes de sécurité ou de fiabilité pour avoir accès aux renseignements classifiés ou protégés, les humains ne se voient normalement pas attribuer de valeurs de confidentialité. Dans quelques rares cas, la divulgation sans autorisation de certaines caractéristiques physiques, comme les empreintes digitales ou autres mesures biométriques, peut causer un préjudice et justifier une catégorisation à des fins de confidentialité. Bien que les renseignements relatifs à un grand nombre de **services** gouvernementaux, comme les données personnelles des clients, puissent avoir des valeurs de confidentialité, les services en tant que tel n'en ont pas. Par exemple, ni la collecte des données du recensement, ni les formulaires connexes ne sont sensibles, du moins jusqu'à ce qu'ils soient remplis. En fait, le service n'a aucune valeur de confidentialité, mais les données en ont une. Dans d'autres cas, la divulgation sans autorisation du service lui-même, comme certains actes médicaux, peut causer un préjudice et par conséquent justifie une catégorisation pour confidentialité.

4.2.3 Disponibilité

> ***Disponibilité*** (*availability*) – condition d'être disponible sur demande afin de soutenir les opérations, les programmes et les services.
>
> *Politique du gouvernement sur la sécurité*, février 2002

La valeur de la disponibilité, c.-à-d. le préjudice qui pourrait vraisemblablement résulter d'une destruction, d'une interruption, d'une suppression ou d'une utilisation sans autorisation, s'applique à tous les **biens**, qu'ils soient corporels ou

incorporels, au **personnel** et aux **services**. Les employés et autres travailleurs sont un cas spécial, parce qu'ils sont susceptibles de se voir attribuer deux valeurs de disponibilité différentes. Du point de vue de la santé et de la sécurité au travail, si l'on examine les risques associés à la violence en milieu de travail et à d'autres menaces directes pour les gens, la valeur intrinsèque d'une personne ou d'un petit groupe est élevée, alors que celle d'un plus grand rassemblement est par définition très élevée. Si les risques ne comprennent pas de dommages physiques directs aux employés et aux autres travailleurs, la valeur de disponibilité attribuée à ces derniers est normalement déterminée par les préjudices probables s'ils étaient incapables de s'acquitter de leurs fonctions. Par exemple, la **valeur de disponibilité intrinsèque** d'un seul commis à la paie serait élevée quelle que soit la tâche qu'il accomplit. Par contre, la **valeur de disponibilité opérationnelle** qui serait attribuée à cette personne serait fonction de l'incidence de son absence sur les fonctions opérationnelles et les clients. Des considérations semblables s'appliquent à la plupart des biens corporels, comme les renseignements, les systèmes de TI et les installations. Leurs valeurs de disponibilité sont généralement fonction de l'importance des services qu'ils soutiennent. Enfin, les valeurs de disponibilité des biens incorporels ont tendance à correspondre à l'incidence psychologique des interruptions de services sur les clients et le grand public.

4.2.4 Intégrité

> ***Intégrité*** (*integrity*) – exactitude et intégralité des biens, et authenticité des transactions.
>
> *Politique du gouvernement sur la sécurité*, février 2002

La valeur de l'intégrité, c.-à-d. le préjudice qui pourrait vraisemblablement résulter d'une modification sans autorisation, s'applique principalement aux **renseignements**. Quelques autres **biens matériels**, comme les instruments de mesure, les systèmes d'alarme ou les capteurs, peuvent aussi être sensibles à une modification sans autorisation qui entraînerait de faux relevés ce qui pourrait avoir des résultats trompeurs ou déconcertants. Bien que le terme intégrité soit fréquemment utilisé pour décrire l'honnêteté ou la fiabilité d'un employé, le **personnel** n'est pas vraiment assujetti aux modifications sans autorisation, de sorte que les gens ne se voient pas attribuer de valeurs d'intégrité dans le contexte de la méthodologie harmonisée d'EMR. Évidemment, toute tentative en vue de miner la loyauté ou la fiabilité d'une personne est un sujet de préoccupation et doit, par conséquent, être examinée durant la phase de l'évaluation des menaces (annexe C), tandis que toute susceptibilité à la subversion ou au recrutement est une caractéristique personnelle qui doit être prise en considération pendant la phase de l'évaluation des vulnérabilités (annexe D). Pour des raisons semblables, les **biens incorporels** ne se voient pas attribuer de valeurs d'intégrité. Inversement, de nombreux **services** peuvent souffrir de la modification sans autorisation de processus ou de procédures, de sorte que ces derniers doivent se voir attribuer des valeurs d'intégrité selon les préjudices probables.

4.2.5 Valeur

> ***Valeur*** (*value*) – coût approximatif soit monétaire, culturel ou autre.
>
> *Politique du gouvernement sur la sécurité*, février 2002

La quatrième mesure de la valeur des biens est, peut-être, la moins utile dans le contexte de la méthodologie harmonisée d'EMR pour plusieurs raisons. La plus importante est que les trois autres échelles de préjudice (confidentialité, disponibilité et intégrité) tiennent compte de tous

les types de préjudices résultant d'une compromission. Par exemple, la valeur monétaire ou le coût de remplacement seraient compris dans le préjudice financier d'une destruction ou d'une suppression sans autorisation. La valeur culturelle d'une peinture ou d'une sculpture même « inestimable » pourrait être exprimée sous l'angle du préjudice psychologique pour la communauté artistique et le grand public en cas de perte, de vol ou de destruction, et sa valeur monétaire, fondée sur le prix qu'elle pourrait obtenir à un encan. Comme les valeurs de confidentialité, de disponibilité et d'intégrité sont attribuées pour correspondre au préjudice maximal auquel on pourrait raisonnablement s'attendre en cas de compromission complète d'un bien, elles ont tendance à être déterminantes dans le calcul des risques résiduels à la suite des évaluation des menaces et des vulnérabilités. Dans quelques cas, cependant, il peut être important de noter la valeur monétaire ou le coût de remplacement d'un bien indépendamment de sa valeur de disponibilité. Habituellement, ce serait le cas si la destruction, l'interruption ou la suppression sans autorisation d'un bien risquait de perturber la prestation de services, causant de ce fait un certain niveau de préjudice physique ou psychologique et une perte financière. Bien qu'il s'agisse là des répercussions les plus graves qui, par conséquent, justifient le plus d'attention dans l'équilibre de l'évaluation, les plus petits risques associés au vol ou aux menus larcins peuvent tout de même devoir être pris en considération sur les plans du préjudice moindre ou du coût de remplacement.

4.2.6 Valeurs multiples

Dans les cas où un bien a plus d'une valeur fondée sur les différents préjudices résultant d'une compromission, les valeurs attribuées peuvent être différentes. Par exemple, la modification sans autorisation d'un dossier médical peut menacer une vie, une valeur d'intégrité élevée, alors que sa divulgation sans autorisation peut causer un embarras grave et inquiéter le public, une valeur de confidentialité moyenne. Par conséquent, pour qu'il soit possible de faire la distinction entre les biens et les valeurs des biens qui contribuent aux plus grands risques, les valeurs de confidentialité, de disponibilité et d'intégrité sont évaluées et attribuées indépendamment pour tous les biens concernés.

4.3 Autres questions

4.3.2 Généralités

Le processus d'évaluation des biens dans un projet d'EMR peut être compliqué par plusieurs considérations secondaires, comme les valeurs changeantes des biens avec le temps, les effets du regroupement et de l'inférence, et certaines conventions administratives ou de sécurité qui, parfois, faussent les valeurs qui ne correspondent plus aux niveaux de préjudice qui pourraient vraisemblablement résulter d'une compromission. Le cas échéant, ces préoccupations peuvent être prises en compte dans l'évaluation des valeurs des biens selon les niveaux de préjudice établis.

4.3.3 Valeurs variables des biens

Les valeurs des biens ne sont pas nécessairement constantes. En fait, elles peuvent varier considérablement au fil du temps, augmentant ou diminuant pour diverses raisons. Par exemple, le budget fédéral se voit attribuer une valeur de confidentialité élevée (Secret) pendant son élaboration, mais dès qu'il est annoncé, la majorité des renseignements qui y sont associés deviennent de notoriété publique. Autrement dit, la valeur de confidentialité chute à très faible

(Non classifié). Il en va souvent de même pour les données de recherche jusqu'à ce que les brevets soient approuvés, les plans militaires jusqu'à ce qu'ils soient exécutés et les négociations commerciales jusqu'à ce qu'elles soient conclues. Dans une moindre mesure, les valeurs de confidentialité peuvent augmenter avec le temps parce que le préjudice résultant d'une divulgation sans autorisation peut augmenter à mesure que les plans ou les programmes mûrissent et que les données pertinentes deviennent plus ciblées ou précises. Les valeurs de disponibilité peuvent aussi être changeantes. Bien qu'une panne de courant généralisée au cours de l'été puisse causer de sérieux préjudices, une interruption de service semblable au milieu de l'hiver pourrait avoir des conséquences désastreuses et entraîner de nombreuses pertes de vies. Les valeurs de disponibilité de certains biens peuvent changer à la hausse ou à la baisse en réaction à différents cycles d'activités, comme la comptabilité de fin d'exercice ou les périodes de congé estival. Les valeurs d'intégrité ont tendance à être plus stables, mais les conséquences d'erreurs ou d'omissions peuvent devenir plus critiques à mesure que les délais approchent parce que les mécanismes de vérification normaux peuvent être trop lents ou trop lourds. Enfin, les valeurs monétaires ou les coûts de remplacement augmentent ou diminuent fréquemment en fonction de la nature des biens. Comme différentes mesures de protection peuvent être nécessaires à mesure que les valeurs des biens changent, il faut noter les mesures élevées et faibles dans la liste d'évaluation des biens ou l'énoncé de sensibilité.

4.3.4 Regroupement et inférence

Comme il est indiqué à la section 6.3 de la *Norme sur l'identification des biens*, le regroupement et l'inférence sont deux facteurs à prendre en considération au moment de catégoriser les biens.

- **Regroupement.** Lorsque le nombre de biens augmente, le préjudice résultant d'une compromission peut augmenter également. Par exemple, la divulgation sans autorisation d'un seul dossier du personnel peut causer un certain embarras à l'intéressé et amener le public à s'inquiéter de la capacité de l'organisation de protéger les renseignements personnels. Si tous les dossiers des ressources humaines (RH) d'un grand ministère étaient divulgués de façon inopportune, cependant, les répercussions négatives pourraient être considérablement pires. Du point de vue de la confidentialité, le regroupement a deux dimensions : la sensibilité a tendance à augmenter avec le nombre de données ajoutées à un dossier, et avec le nombre de dossiers réunis dans un fichier ou une base de données. Dans chaque cas, la valeur de confidentialité de l'ensemble peut être plus grande que celle de ses diverses parties en raison du préjudice accru que causerait leur divulgation sans autorisation. Le regroupement s'applique aussi aux valeurs de disponibilité et d'intégrité. Par exemple, la destruction d'un bien, un seul véhicule par exemple, peut avoir des conséquences clairement définies, alors que la perte de tout un parc serait beaucoup plus sérieuse. La modification sans autorisation d'un seul dossier ou la corruption complète d'une grande base de données serait l'équivalent sur le plan de l'intégrité.

> ***Regroupement*** *(aggregation)* – situation où un ensemble de biens peuvent être catégorisés à un niveau de sensibilité plus élevé que les parties qui le forment en raison du préjudice accru que pourrait causer toute compromission à ce bien. Le regroupement s'applique généralement à la confidentialité, mais, dans certains cas, il peut également s'appliquer à la disponibilité et à l'intégrité.
>
> Section 2, Norme *Identification des biens*

Dans chaque cas, la *Méthodologie harmonisée d'EMR* facilite l'analyse de valeurs de biens qui augmentent avec le regroupement parce que les niveaux gradués présentés dans l'appendice B-4, Tableau détaillé des préjudices, peuvent être appliqués en toute confiance pour catégoriser des biens individuels ou des groupes importants et ce, de façon précise et constante sans en sous-estimer ou surestimer la valeur.

- **Inférence.** De par sa nature même, l'inférence ne s'applique qu'à la confidentialité, parce que l'accès à des données en apparence inoffensives dont la sensibilité est faible ou nulle peut permettre à une personne avertie de tirer des conclusions beaucoup plus préjudiciables sur les capacités ou les intentions d'une autre organisation. Par exemple, l'étude des mouvements de personnel afin d'identifier les qualifications et les affiliations des cadres supérieurs ou d'autres employés sélectionnés pour différents postes peut fournir des indicateurs utiles de futurs programmes stratégiques ou plans opérationnels. Malheureusement, la relation entre différentes données et sources de données peut être très subtile, ténue même, de sorte que les occasions d'inférence sont généralement beaucoup plus difficiles à identifier et à évaluer. Néanmoins, lorsque la possibilité existe, le tableau gradué des préjudices permet une évaluation objective des biens faisant l'objet de conclusions inférées. D'un point de vue pratique, l'inférence doit être évaluée avec prudence, car les scénarios complexes peuvent exagérer le risque et donner lieu à une surclassification inutile.

> ***Inférence*** *(inference)* – situation où l'analyse de biens catégorisés à un certain niveau de sensibilité permet de conclure qu'il existe un risque de préjudice plus élevé.
>
> Section 2, Norme *Identification des biens*

4.3.5 Conventions d'évaluation des biens

Dans certains cas, les valeurs de biens sur le plan de la confidentialité sont attribuées en fonction de conventions administratives ou opérationnelles plutôt que d'une application scrupuleuse des critères de préjudice. Par exemple, les dossiers et les ébauches qui constituent des renseignements confidentiels du Conseil privé de la Reine pour le Canada et entrent dans le Système des dossiers du Cabinet sont habituellement classifiés Secret[4], une valeur élevée, quel que soit le préjudice réel qui pourrait vraisemblablement résulter d'une divulgation sans autorisation. Beaucoup de renseignements personnels sont catégorisés Protégé B, une valeur moyenne, même dans les cas où le préjudice risquant le plus de résulter d'une divulgation sans autorisation pourrait être un léger embarras ou de la frustration. De même, certains plans opérationnels ou documents du renseignement sont automatiquement classifiés Secret et Très secret sans que l'on tienne compte des conséquences probables d'une compromission. Bien que le strict respect de ces conventions puisse élever artificiellement les niveaux évalués de risques résiduels d'un projet d'EMR, les règles ne doivent pas être remises en question. Dans quelques rares cas, cependant, il peut être utile de réévaluer les risques résiduels en utilisant des valeurs de biens plus réalistes pour déterminer si d'autres mesures de protection pourraient être plus appropriées dans les circonstances.

[4] Voir l'appendice B de la *Norme opérationnelle de sécurité – Identification des biens*.

5 Tableau priorisé d'évaluation des biens / Énoncé de sensibilité

Comme il est indiqué ci-dessus, chaque bien inclus dans la portée du projet d'EMR doit se voir attribuer une ou plusieurs valeurs selon le préjudice maximal qui pourrait vraisemblablement résulter d'une compromission. Les valeurs de confidentialité font état des conséquences les plus graves d'une divulgation sans autorisation; les valeurs de disponibilité correspondent aux répercussions éventuelles d'une destruction, d'une interruption, d'une suppression ou d'une utilisation sans autorisation; alors que les valeurs d'intégrité témoignent des pires effets d'une modification sans autorisation. Dans certains cas, des valeurs monétaires ou coûts de remplacement peuvent être inscrites séparément à des fins d'analyse. Pour plus de raffinement, les valeurs des biens qui se situent près de la limite entre deux niveaux peuvent être mises en évidence pour être réexaminées au moment du calcul final des risques résiduels[5]. Puis, toutes ces valeurs doivent être consignées dans un tableau d'évaluation des biens, aussi appelé « énoncé de sensibilité », le résultat final de la phase d'identification et d'évaluation des biens d'un projet d'EMR. Un simple tri par valeurs des biens, de Très faible à Très élevé, permet de rapidement classer les biens par ordre de priorité et d'identifier ceux qui ont le plus de valeur.

Cette liste est illustrée dans le tableau B-4 et développée dans l'appendice B-5.

Classe	Catégorie	Groupe	Sous-groupe	Composante	C	D[6]		I	$
						In	Op		
Légende C – Valeur de confidentialité. D – Valeur de disponibilité. In – Valeur de disponibilité intrinsèque pour le personnel. Op – Valeur de disponibilité opérationnelle pour le personnel. I – Valeur d'intégrité. $ - Coût de remplacement.									

Tableau B-4 : Exemple de tableau d'évaluation des biens/énoncé de sensibilité

[5] Voir la section 2.4.3 de l'annexe E pour obtenir une explication de cette possibilité.

[6] Comme il est indiqué dans la section 4.2.2, les employés peuvent se voir attribuer deux valeurs de biens pour la disponibilité : une valeur intrinsèque (In) s'il y a des menaces de violence et une valeur opérationnelle (Op) correspondant à l'incidence de leur absence sur la prestation des services.

Page intentionnellement laissée en blanc

Appendice B-1 - Sources de données sur les biens

RESSOURCES MINISTÉRIELLES	
Source de données	**Type de bien**
• Gestionnaires de programme	• Plans d'activités/services • Employés • Équipement/fournitures de bureau • Budget/Finances • Rapports de R et D
• Gestionnaires de projet	• Documentation sur la conception • Plans d'étage • Schémas de l'équipement/plans de recolement • Procédures opérationnelles
• Gestionnaires du matériel/des biens	• Répertoires • Documentation sur les marchés • Véhicules
• Gestionnaires des installations	• Plans des immeubles • Services d'urgence o Service d'incendie o Ambulanciers paramédicaux o Service de police • Systèmes de chauffage, de ventilation et de climatisation • Mesures de sécurité matérielle o Alarmes o Contrôles d'accès • Services publics o Électricité o Égouts o Eau
• Ressources humaines	• Employés • Postes/qualités approuvés • Renseignements personnels
• Finances	• Budgets • Coûts des programmes
• Dirigeant principal de l'information	• Infrastructure des TI • Applications communes/partagées
• Administrateur (de la sécurité) des systèmes	• Configurations du matériel/des logiciels • Mesures de sécurité techniques
• Vérification et examen	• Rapports de vérification/examens
• Agent de sécurité du ministère	• Mesures de sécurité matérielle

RESSOURCES MINISTÉRIELLES	
Source de données	**Type de bien**
	• Plans/inspections de sécurité
• Coordonnateur de la sécurité des TI	• Mesures de sécurité techniques
• Coordonnateur, PCA	• Analyse des répercussions sur les opérations
• Coordonnateur de l'AIPRP	• Évaluations des facteurs relatifs à la vie privée
• Agent de santé et de sécurité au travail	• Équipement/procédures de santé et de sécurité

RESSOURCES EXTERNES	
Source des données	**Type de bien**
• Gardiens d'immeuble	• Plans des immeubles • Systèmes de chauffage, de ventilation et de climatisation • Services publics • Mesures de sécurité matérielle/alarmes/contrôles d'accès
• Services publics	• Services d'électricité/d'eau
• Services d'urgence	• Service d'incendie/de police/ambulanciers paramédicaux
• Fournisseurs de services	• Infrastructure des communications
• Fournisseurs de produits	• Descriptions/spécifications/schémas des produits
• Clients	• Produits et services

Nota : Cette liste n'est pas exhaustive. Elle se veut seulement un point de départ utile aux fins de la collecte des données. D'autres éléments y seront ajoutés et explicités à l'occasion. Toute suggestion de documents de référence ou de contacts à ajouter peut être présentée aux bureaux mentionnés dans l'Avant-propos.

Appendice B-2 - Liste des biens

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
Personnes	Employés	Cadres supérieurs		
		Personnel de programme	Gestionnaires	
			Superviseurs	
			Analystes des systèmes de gestion	
			Ingénieurs	
			Scientifiques	
			Travailleurs de la production	
		Analystes des politiques		
		Spécialistes du marketing		
		Communications		
		Conseillers juridiques		
		Vérificateurs		
		Gestion de projet	Directeur de projet	
			Gestionnaire de projet	
			Architectes de systèmes	
			Programmeurs d'applications	
			Ingénieurs en matériel informatique	
			Rédacteurs techniques	
		Personnel des TI	Administrateurs de systèmes	
			Administrateurs de la sécurité	
			Responsables de la maintenance des logiciels	
			Techniciens de matériel informatique	
			Analystes en assistance technique	
		Personnel de soutien	Adjoints administratifs	
			Personnel chargé de la gestion des dossiers	
			Chauffeurs	
			Messagers	
		Traducteurs		
		Gestion des installations	Gestionnaire d'immeuble	
			Préposés au nettoyage	
			Électriciens	
			Techniciens des systèmes CVC	
			Plombiers	
		Finances	Comptables	
			Commis aux comptes créditeurs	
			Commis aux comptes débiteurs	
		Ressources humaines	Classification	

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
			Dotation	
			Relations de travail	
			Formateurs	
			Aide aux employés	
		Santé et sécurité au travail	Analystes	
			Enquêteurs	
		Personnel chargé des PCA		
		Renseignement	Analyste du renseignement	
			Compilateur	
		Sécurité	Gestion	
			Analystes	
			Planification de la continuité des activités	
			Enquêteurs/inspecteurs	
			Personnel de la sécurité des TI	
			Gardien COMSEC	
			Gardes	
			Opérateur de console de système d'alarme	
	Entrepreneurs	(n'importe laquelle des valeurs ci-dessus)		
	Sous-traitants	(n'importe laquelle des valeurs ci-dessus)		
	Fournisseurs de produits	(n'importe laquelle des valeurs ci-dessus)		
	Fournisseurs de services	(n'importe laquelle des valeurs ci-dessus)		
	Autres gouvernements	(n'importe laquelle des valeurs ci-dessus)		
	Organismes alliés	(n'importe laquelle des valeurs ci-dessus)		
	Établissements d'enseignement	(n'importe laquelle des valeurs ci-dessus)		
	Clients			
	Public			
Biens corporels	Information	Renseignements personnels	Employés	Identification
				Études et formation
				Autres qualités
				Antécédents d'emploi
				Évaluations du rendement
				Dossiers disciplinaires
				Antécédents médicaux
				Rémunération et avantages sociaux
				Relevés de congé
				Dossier d'enquête sur la sécurité
				Casiers judiciaires
			Clients	Identification

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
				Revenu
				Antécédents de crédit
				Antécédents de transaction
				Soldes de comptes
		Documents du Cabinet		
		Politiques/Normes	Politiques fédérales	Politique du gouvernement sur la sécurité
				Politique sur l'accès à l'information
				Politique sur l'équité en emploi
				Politique sur la protection des renseignements personnels
				Autres politiques
			Normes fédérales (sécurité)	Planification de la continuité des activités
				Identification des biens
				Gestion de la sécurité des TI
				Sécurité matérielle
				Niveaux de préparation
				Sécurité des marchés
				Loi sur la protection de l'information
				Gestion des risques liés à la sécurité
				Filtrage de sécurité
				Formation et sensibilisation en matière de sécurité
			Politiques ministérielles	Sécurité
				Autre
		Plans d'activités	Stratégies opérationnelles	
			Plans de marketing	
			Listes de clients	
		Dossiers financiers	Plans des dépenses	
			Rapports annuels	
			Registres de paye	Salaires
				Avantages sociaux
			Budget de F et E	Déplacements
				Fournitures
			Tarification des services	
			Transactions	Comptes fournisseurs
				Comptes créditeurs
			Budget d'immobilisations	Équipement des TI
				Autre matériel
		Correspondance courante		
		Rapports de vérification	Vérifications internes	
			Examens	
		Documentation des projets		
		Documents d'architecture		
		Documentation des systèmes	Manuels des fournisseurs	
		Données scientifiques ou techniques	Propositions de R et D	

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
			Comptes rendus de recherche	
			Données expérimentales	
		Dossiers juridiques	Dossiers des poursuites	Poursuites civiles
				Poursuites criminelles
			Opinions juridiques	
			Marchés	
			Protocoles d'entente	Partage de l'information
				Échelle internationale
				Autres gouvernements
				Secteur privé
		Casiers judiciaires	Rapports d'enquête	
			Déclarations de témoins	
			Casiers judiciaires	Fichiers d'empreintes digitales
			Éléments de preuve	
		Rapports de renseignement	De nature politique	
			De nature économique	
			Sécurité	Services de renseignement
				Activités pour le compte d'une entité étrangère
				Terrorisme
			De nature criminelle	
			Sources ouvertes	
		Information sur des tiers	Organismes alliés	
			Autres gouvernements	Provincial
				Municipal
			Infrastructures essentielles	Établissements financiers
				Secteur de la santé
				Services publics
				Secteur des télécommunications
				Secteur des transports
			Autres, secteur privé	Non-divulgation (fournisseurs)
				Secrets commerciaux
	Matériel informatique	Processeurs	Super-ordinateurs	
			Ordinateurs centraux	
			Mini-ordinateurs	
			Serveurs	
			Ordinateurs personnels	Unité de disque dur
				Puces mémoire
				Coprocesseur mathématique
				Carte réseau
				Clavier
				Écran
				Souris
				Haut-parleurs
			Ordinateurs portatifs	
			Assistants numériques personnels	Dispositifs Blackberry
		Périphériques	Imprimantes	
			Scanners	
			Chargeurs de disques	

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
		Composantes réseau	Routeurs	
			Concentrateurs	
			Câblage	Fibre optique
				Câble coaxial
				Câble à paires torsadées
			Garde-barrière	
			Dispositifs sans fil	
		Composantes de sécurité	Dispositifs cryptographiques	
			Équipement biométrique	Lecteur d'empreintes rétiniennes
				Lecteur d'empreintes digitales
			Technologies des cartes évoluées	
			Dispositifs d'accès à distance sécurisés	
		Supports	Bandes	
			Disquettes	
			CD	
			DVD	
			CD-ROM	
			Unités USB	
			Disques durs	
	Micrologiciels			
	Logiciels	Systèmes d'exploitation	Windows NT	Version/Correctif
			Windows XP	Version/Correctif
			Linux	Version/Correctif
			Solaris	Version/Correctif
		Applications commerciales	Bureautique	Microsoft Word
				Microsoft PowerPoint
				Microsoft Excel
				Corel WordPerfect
				Lotus WordPro
			Messagerie électronique	Microsoft Outlook
			Navigateurs Web	Microsoft Internet Explorer
				Netscape Communicator
			Progiciels graphiques	Corel Draw
				Adobe Illustrator/Photoshop
				AutoCad
		Applications personnalisées	Systèmes financiers	Code source
				Code objet
			Systèmes du personnel	Code source
				Code objet
			Gestion du matériel	Code source
				Code objet
		Utilitaires de sécurité	Progiciels de chiffrement	Entrust
				PGP
				SecureDoc
			Logiciels antivirus	McAfee VirusScan
				Norton AntiVirus
			Systèmes de détection des intrusions	Sur réseau
				Sur hôte

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
			Systèmes de prévention des intrusions	Sur réseau
				Sur hôte
		Logiciels tierce partie/logiciels loués	(n'importe laquelle des valeurs ci-dessus)	
		Partagiciels	(n'importe laquelle des valeurs ci-dessus)	
		Gratuiciels	(n'importe laquelle des valeurs ci-dessus)	
	Installations	Immeubles	Locaux à bureaux	Bureaux fermés
				Bureaux à aire ouverte
				Aires de réception
				Locaux de réunion sécurisés
				Chambres fortes
				Enceintes blindées
			Centres de données	
			Armoires de câblage	
			Installations médicales	Cabinets de médecin
				Locaux pour les patients
				Salles d'opération
				Entreposage médical (médicaments)
			Stockage et entreposage	
			Laboratoires	
			Installations de sécurité	Centres des opérations
				Centres de protection de l'information
				Postes de garde
		Systèmes de chauffage, de ventilation et de climatisation	Systèmes de chauffage	
			Ventilateurs	
			Climatisation	
		Réseaux de plomberie		
		Réseaux électriques	Câblage	
			Coupe-circuits	
		Mobilier de bureau	Bureaux	
			Chaises	
			Armoires de rangement	
		Autre équipement de bureau	Photocopieurs	Non résidents en mémoire
				Résidents en mémoire
			Télécopieurs	Non résidents en mémoire
				Résidents en mémoire
			Téléphones	De bureau
				Cellulaires
		Fournitures de bureau	Papeterie	
			Formulaires préimprimés	
	Dispositifs de sécurité	Systèmes d'alarme	Alarmes anti-intrusion	Détecteurs de secteur
				Interrupteurs de contact
				Consoles de surveillance
			Détecteurs de fumée	

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
			Avertisseurs d'incendie	
		Contenants de sécurité		
		Serrures		
		Déchiqueteurs		
		Dispositifs cryptographiques		
		Équipement biométrique	Lecteur d'empreintes rétiniennes	
			Lecteur d'empreintes digitales	
		Technologies des cartes évoluées		
	Processus	Processus opérationnels		
		Processus de conception des systèmes	Gestion de la capacité	
			Gestion des changements	
			Gestion des configurations	
			Gestion des correctifs	
			Gestion des versions	
			Cycle de développement de système	Planification des changements
				Définition des besoins
				Conception architecturale
				Conception détaillée
				Mise en œuvre
				Tests et évaluation
		Processus de sécurité	Gestion de l'accès	
			Autorisation	
			Planification de la continuité des activités	
			Identification et authentification	
			Certification et accréditation	Programmes ministériels
				Services partagés/communs
			Traitement des incidents de sécurité	
		Procédures opérationnelles	Processus manuels	
			Instructions pour l'exploitation des TI	
			Plans de gestion des configurations	
			Procédures d'urgence	
	Autres	Véhicules	Véhicules à passagers	
			Camions	Camionnettes
				Camions lourds
			Chariots élévateurs	
			Véhicules tout-terrain	
			Véhicules de secours	Ambulances
				Voitures de patrouille
				Camions incendie
				Équipement de déneigement
			Matériel de construction	Bulldozers
				Niveleuses
				Pelles rétrocaveuses

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
				Grues
			Prototypes	
		Navires/bateaux		
		Aéronefs		
		Fournitures médicales	Médicaments	Médicaments
				Vaccins
			Équipement médical	
		Matières dangereuses	Liquides combustibles	
			Gaz comprimés	
			Produits chimiques corrosifs	
			Aérosols inflammables	
			Gaz inflammables	
			Liquides inflammables	
			Agents réactifs inflammables	
			Solides inflammables	
			Oxydants	
			Agents réactifs	
	Instruments négociables	Espèces	Devises canadiennes	
			Devises étrangères	
		Chèques		
		Obligations		
		Pierres précieuses		
		Métaux précieux		
Services	Services gouvernementaux	Agriculture et Agroalimentaire	(Secteurs d'activité ministériels)	
		Patrimoine	(Secteurs d'activité ministériels)	
		Citoyenneté et Immigration	(Secteurs d'activité ministériels)	
		Environnement	(Secteurs d'activité ministériels)	
		Finances	(Secteurs d'activité ministériels)	
		Pêches et Océans	(Secteurs d'activité ministériels)	
		Affaires étrangères	(Secteurs d'activité ministériels)	
		Commerce international	(Secteurs d'activité ministériels)	
		Ressources humaines	(Secteurs d'activité ministériels)	
		Affaires indiennes	(Secteurs d'activité ministériels)	
		Développement du Nord	(Secteurs d'activité ministériels)	
		Industrie	(Secteurs d'activité ministériels)	
		Justice	(Secteurs d'activité ministériels)	
		Défense nationale	(Secteurs d'activité ministériels)	
		Ressources naturelles	(Secteurs d'activité ministériels)	
		SPPCC	(Secteurs d'activité ministériels)	
		TPSGC	(Secteurs d'activité ministériels)	
		Transports	(Secteurs d'activité ministériels)	
		Conseil du Trésor	(Secteurs d'activité ministériels)	
		Affaires des Anciens combattants	(Secteurs d'activité ministériels)	
		Services de réseau	Réseau local d'entreprise	
			Accès à distance	
			Accès sans fil	
			Services Internet	Haute vitesse
				Accès commuté

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel
		Services partagés du GC		
	Services environnementaux	Services publics	Électricité	
			Eau	
			Égouts	
			Gaz naturel	
			Enlèvement des ordures	
			Déneigement	
			Entretien des routes	
		Télécommunications	Téléphone	
			Télévision	Câblodistribution
			Autres TI	Sociétés de services informatiques
				Consultants
		Services d'urgence	Service de police	Fédéral
				Provincial
				Municipal
			Service d'incendie	
			Services médicaux	Ambulances
				Ambulanciers paramédicaux
Biens incorporels	Internes	Moral des employés		
		Confiance des employés		
		Crédibilité de la gestion		
	Externes	Confiance du public		
		Avantage concurrentiel		
		Identité du produit		
		Crédibilité de l'organisme		

Nota :

1. De toute évidence, la liste des biens n'est pas exhaustive et ne pourra jamais l'être. De nouveaux biens apparaissent régulièrement, en particulier au niveau de ventilation des composants. Par conséquent, d'autres éléments seront ajoutés occasionnellement à la liste. Toute suggestion d'ajout peut être présentée aux bureaux mentionnés dans l'Avant-propos.
2. Lorsqu'un énoncé de sensibilité est établi dans le cadre d'un projet d'EMR, tous les biens visés par l'évaluation peuvent être transférés, au niveau de ventilation qui convient, de la liste ci-dessus aux cinq premières colonnes du tableau d'évaluation des biens/énoncé de sensibilité à l'appendice B-5.

Page intentionnellement laissée en blanc

Appendice B-3 - ARO, EFVP et EMR

1 Introduction

1.1 Généralités

L'analyse des répercussions sur les opérations (ARO), mentionnée à la section 10.14 de la PGS, Planification de la continuité opérationnelle, et l'évaluation des facteurs relatifs à la vie privée (EFVP), mentionnée dans la politique de l'EFVP, sont des exigences obligatoires de la PGS. À titre de processus analytique, l'ARO et l'EFVP ont des objectifs comparables à l'EMR. Une bonne compréhension des similitudes et des différences entre ces trois activités interreliées peut améliorer l'utilité et l'efficacité de ces disciplines complémentaires.

1.2 But

Le double but de cet appendice est de comparer et de mettre en relief l'objectif, la portée et le contenu de l'ARO, de l'EFVP et de l'EMR, et de proposer une façon de les appliquer de manière coordonnée.

2 Objectif

Selon la PGS et la politique de l'EFVP, les trois activités ont des objectifs similaires malgré quelques différences particulières. Les principaux buts de chaque processus peuvent être résumés comme suit :

- **ARO** – « inventorier par ordre de priorité les services et les biens essentiels. »[1]
- **EFVP** – s'assurer de « tenir compte des questions de protection de la vie privée à toutes les étapes de la conception ou de la refonte des programmes et des services » et « garantir que tous les problèmes touchant le respect de la vie privée ont été cernés et réglés ou atténués. »[2]
- **EMR** – « déterminer la nécessité d'aller au-delà des mesures sécuritaires de base. »[3]

En bref, les trois processus prévoient un élément d'analyse pour appuyer les recommandations concernant toute mesure éventuelle relative aux différents risques. La liste priorisée des services et biens essentiels d'une ARO offre une base objective pour la sélection de plans, de mesures et de préparatifs appropriés de la PCA pour remédier aux risques liés à la disponibilité. D'une manière semblable, l'EFVP aide les autorités responsables à prendre des décisions pleinement éclairées en matière de politique, de conception de système et d'approvisionnement dans le but d'éviter ou d'atténuer les risques d'entrave à la vie privée. Enfin, l'EMR identifie les risques inacceptables envers les employés, les biens et la prestation des services et recommande des

1 PGS, section 10.14 b).
2 Politique de l'EFVP, page 2.
3 PGS, section 10.7.

mesures supplémentaires de protection au delà des contrôles de base pour obtenir des solutions de sécurité rentables.

3 Portée

3.1 Généralités

Bien que l'ARO, l'EFVP et l'EMR soient des méthodes analytiques complémentaires qui permettent d'évaluer et, ultimement, d'atténuer divers risques, leur portée peut être très différente.

3.2 Portée d'une EMR

En général, l'EMR englobe un plus large éventail de biens et de valeurs de biens que l'ARO ou l'EFVP. Selon l'objet de l'évaluation, une EMR peut analyser les risques auxquels sont exposés tous les biens (corporels, incorporels, personnel et services) et les valeurs de biens (confidentialité, intégrité et disponibilité), tel qu'il est illustré dans la figure B3-1.

<table>
<tr><th></th><th colspan="2">Biens corporels</th><th rowspan="2">Biens incorporels</th><th rowspan="2">Personnel</th><th rowspan="2">Services</th></tr>
<tr><th></th><th>Information</th><th>Autres</th></tr>
<tr><td>Confidentialité</td><td></td><td></td><td colspan="3" rowspan="2">Non applicables à tous les cas[4]</td></tr>
<tr><td>Intégrité</td><td></td><td></td></tr>
<tr><td>Disponibilité</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure B3-1: Portée d'une EMR

3.3 Portée d'une ARO

Pour identifier les biens et les services critiques, l'ARO met l'accent sur la disponibilité et, dans une moindre mesure, l'intégrité des valeurs de biens dont la compromission (destruction, suppression, modification, interruption ou utilisation non autorisées) est susceptible de causer de graves préjudices. Évidemment, les préoccupations concernant la confidentialité doivent être abordées lors de la sélection et de la mise en œuvre subséquentes des plans, des mesures et des préparatifs de la PCA; néanmoins, l'ARO met avant tout l'accent sur les biens dont les valeurs de disponibilité sont élevées et très élevées, tel qu'il est illustré dans la figure B3-2.

[4] Comme il est expliqué à la section 4.2 de l'annexe B, Phase d'identification et d'évaluation des biens, les valeurs de confidentialité et d'intégrité ne s'appliquent pas normalement au personnel, aux services et aux biens incorporels.

<table>
<tr><th></th><th colspan="2">Biens corporels</th><th rowspan="2">Biens incorporels</th><th rowspan="2">Personnel</th><th rowspan="2">Services</th></tr>
<tr><th></th><th>Information</th><th>Autres</th></tr>
<tr><td>Confidentialité</td><td></td><td></td><td colspan="3" rowspan="2">Non applicables à tous les cas[5]</td></tr>
<tr><td>Intégrité</td><td></td><td></td></tr>
<tr><td rowspan="2">Disponibilité</td><td colspan="5">Biens et services essentiels</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure B3-2: Portée d'une ARO

3.4 Portée d'une EFVP

L'EFVP s'applique uniquement aux programmes et aux services qui traitent les renseignements personnels, sous-ensembles importants mais limités des biens corporels. Les autres renseignements, les installations, le personnel, les services et les biens incorporels ne sont généralement pas inclus dans la portée de l'évaluation. Contrairement à l'ARO, toutefois, l'EFVP tient compte des trois dimensions des valeurs de biens et évalue les risques qui menacent la confidentialité et l'intégrité ainsi que la disponibilité, tel qu'il est illustré dans la figure B3-3.

<table>
<tr><th></th><th colspan="3">Biens corporels</th><th rowspan="2">Biens incorporels</th><th rowspan="2">Personnel</th><th rowspan="2">Services</th></tr>
<tr><th></th><th colspan="2">Information</th><th>Autres</th></tr>
<tr><td>Confidentialité</td><td rowspan="3">Rens. personnels</td><td></td><td></td><td colspan="3" rowspan="2">Non applicables à tous les cas[6]</td></tr>
<tr><td>Intégrité</td><td></td><td></td></tr>
<tr><td>Disponibilité</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Figure B3-3: Portée d'une EFVP

[5] Comme il est expliqué à la section 4.2 de l'annexe B, Phase d'identification et d'évaluation des biens, les valeurs de confidentialité et d'intégrité ne s'appliquent pas normalement au personnel, aux services et aux biens incorporels.

[6] Comme il est expliqué à la section 4.2 de l'annexe B, Phase d'identification et d'évaluation des biens, les valeurs de confidentialité et d'intégrité ne s'appliquent pas normalement au personnel, aux services et aux biens incorporels.

4 Contenu

4.1 Processus analytique

4.1.1 ARO

L'ARO est le deuxième de cinq éléments d'un programme de PCA décrits à la section 10.14 de la PGS. Les autres éléments incluent la structure de régie, les plans et préparatifs, le niveau de préparation du programme et les activités permanentes de revue, de mise à l'essai et de vérification. La section 3.2 de la *Norme opérationnelle de sécurité – Programme de planification de la continuité des activités (PCA)* identifie les cinq étapes de l'ARO qui visent à établir une base solide pour les recommandations subséquentes concernant des plans, des mesures et des préparatifs appropriés de PCA. Tel qu'il est indiqué dans le tableau B3-1, ces cinq étapes (Déterminer la nature des activité du ministère et des services, Déterminer les répercussions des interruptions, Déterminer les services susceptibles de causer un préjudice élevé, Relever les services essentiels et les classer par ordre de priorité, et Obtenir l'approbation de la haute direction) se rapprochent beaucoup de la composante d'analyse des données d'une EFVP et de la phase d'identification/évaluation des biens d'une EMR. Donc, l'ARO elle-même est une activité beaucoup plus restreinte que l'EFVP ou l'EMR. Cela dit, pour établir un meilleur parallèle, les autres éléments d'un programme de PCA complet, telle la sélection des plans et des préparatifs, correspondent à la conclusion et aux étapes suivantes d'une EFVP et à la phase des recommandations d'une EMR. Enfin, un programme de PCA n'a pas d'équivalent pour les phases d'évaluation des menaces et des risques d'une EMR puisque l'inévitabilité des incidents perturbateurs est une hypothèse sous-jacente durant tout le processus analytique.

4.1.2 EFVP

Le document *Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée - Cadre de gestion des risques d'entrave à la vie privée* prescrit un processus d'EFVP en quatre étapes : (1) Lancement du projet, (2) Analyse des données, (3) Analyse des facteurs relatifs à la vie privée et (4) Évaluation des facteurs relatifs à la vie privée. Un examen des activités subordonnées de chaque étape révèle que le lancement du projet est presque identique à la phase de préparation d'une EMR. L'analyse des données correspond étroitement à la phase d'identification et d'évaluation des biens. Comme dans le cas de l'ARO, il n'y a pas d'équivalent pour la phase d'évaluation des menaces, mais l'analyse des facteurs relatifs à la vie privée est semblable aux phases d'évaluation des risques et des recommandations d'une EMR. Donc, l'objectif et la portée d'une EFVP sont certainement plus ciblés que ceux d'une EMR; toutefois, une forte ressemblance demeure entre les processus analytiques d'évaluation et d'atténuation des risques.

4.1.3 EMR

La phase d'évaluation des menaces unique et l'évaluation des vulnérabilités plus explicite d'une EMR typique font en sorte que cette méthode demande plus de temps et traite davantage de détails que l'ARO ou l'EFVP. Néanmoins, le calcul des risques résiduels et la phase des recommandations correspondent d'assez près à l'étape d'évaluation des facteurs relatifs à la vie privée d'une EFVP et à l'élément des plans et préparatifs d'un programme de PCA. Tel qu'il est indiqué ci-dessus, ces interrelations sont illustrées dans le tableau B3-1.

Programme de PCA	EFVP	EMR
Régie de PCA • Former le comité de gestion • Nommer le coordonnateur de la PCA	Lancement du projet • Définir la portée du processus d'EFVP • Nommer les ressources de l'équipe • Adapter les outils pour tenir compte de la portée	Phase de préparation • Établir le mandat de l'EMR • Déterminer la portée de l'évaluation • Choisir l'équipe d'EMR • Préparer un ébauche du plan de travail de l'EMR
Analyse des répercussions sur les opérations (ARO) • Déterminer la nature des activité du ministère et des services • Déterminer les répercussions des interruptions • Déterminer les services susceptibles de causer un préjudice élevé • Relever les services essentiels et les classer par ordre de priorité • Obtenir l'approbation de la haute direction	Analyse des données • Décrire les processus opérationnels • Identifier les renseignements personnels • Développer les diagrammes de données	Identification et évaluation des biens • Identifier les biens • Effectuer des évaluations des préjudices • Attribuer des valeurs de biens
		Évaluation des menaces • Identifier les menaces • Déterminer la probabilité des menaces • Évaluer la gravité des menaces • Attribuer les niveaux de menace
	Analyse des facteurs relatifs à la vie privée • Remplir les questionnaires • Analyser et clarifier • Décrire les problèmes/ répercussions	Évaluation des risques Évaluation de la vulnérabilité • Recenser les mesures de protection • Évaluer l'efficacité des mesures de protection • Identifier les vulnérabilités • Analyser les incidences des vulnérabilités • Attribuer les niveaux de vulnérabilité

Programme de PCA	EFVP	EMR
	Évaluation des facteurs relatifs à la vie privée • Résumer les risques d'entrave à la vie privée	Évaluation des risques: Calcul des risques résiduels • Calculer les risques résiduels • Prioriser les risques résiduels
Plans de PCA et préparatifs • Élaborer des options de reprise • Évaluer les avantages/coûts • Obtenir l'approbation de la haute direction • Élaborer des plans de continuité des activités • Informer/former le personnel	• Identifier les mesures d'atténuation • Conclusion et prochaines étapes	Recommandations • Identifier les risques inacceptables • Sélectionner des mesures de protection potentielles • Identifier les coûts connexes • Évaluer les risques résiduels projetés
État de préparation du programme de PCA • Examen/révision continus • Formation supplémentaire • Mises à l'essai/validations régulières • Cycle de vérification/rapport au SCT		

Tableau B3-1: Processus comparatif de mise en correspondance de l'ARO, de l'EFVP et de l'EMR

4.2 Paramètres comparatifs

Bien que l'ARO comprenne une estimation des niveaux de service minimaux et un temps d'arrêt permis maximal, elle ne définit pas explicitement la mesure finale de la valeur de disponibilité, un haut niveau de préjudice. De la même manière, l'EFVP ne prescrit pas d'échelles graduées pour la sensibilité des renseignements personnels ni pour les risques connexes d'entrave à la vie privée. Réciproquement, la méthodologie harmonisée d'EMR prévoit des paramètres clairs pour les valeurs de biens, les menaces, les vulnérabilités et les risques résiduels afin de favoriser une analyse objective.

5 Application complémentaire

5.1 Éléments d'entrée et de sortie

5.1.1 L'ARO/EFVP comme éléments d'entrée dans une EMR

Tant l'ARO que l'EFVP peuvent constituer des éléments d'entrée précieux dans un projet d'EMR, en particulier la phase d'identification et d'évaluation des biens, tel qu'il est indiqué aux sections 5.4.6 et 5.5.1 de l'annexe A. Les réponses aux questionnaires A et B dans l'étape d'analyse des facteurs relatifs à la vie privée d'une EFVP peuvent également fournir de

l'information utile pour l'évaluation des vulnérabilités, tout comme les facteurs d'atténuation ou les mesures de protection précisés dans l'étape finale de l'EFVP.

5.1.2 L'EMR comme élément d'entrées dans une ARO/EFVP

En l'absence d'une ARO ou d'une EFVP, les données recueillies au cours d'un projet d'EMR peuvent être assemblées pour produire les autres documents connexes, en particulier lorsque l'objectif est clairement défini dès le départ. Par exemple, l'énoncé de sensibilité d'un rapport d'EMR doit fournir suffisamment d'information pour permettre la compilation à la fois d'une ARO et de l'étape d'analyse des données d'une EFVP. Ensuite, l'évaluation des vulnérabilités et la phase des recommandations doivent inclure une analyse approfondie des mesures de protection de la disponibilité, incluant les plans de PCA et les préparatifs, troisième élément d'une programme de PCA complet. De la même manière, l'information recueillie pour l'évaluation des vulnérabilités doit tenir compte de la plupart des questions des questionnaires A et B de l'étape d'analyse des facteurs relatifs à la vie privée d'une EFVP, en particulier celles qui concernent les principes de protection de la vie privée suivants : (5) communication et retrait des renseignements personnels, (6) exactitude des renseignements personnels, (7) protection des renseignements personnels et (9) accès aux renseignements personnels.

5.2 Analyse comparative

Les paramètres concrets de l'EMR offrent de réelles possibilités de raffiner l'ARO et l'EFVP et de faciliter la priorisation de la PCA et des risques d'entrave à la vie privée. Cette capacité d'analyse comparative peut être particulièrement utile pour l'attribution de ressources limitées lors de l'établissement des plans, des mesures et des préparatifs de PCA ou de la sélection des mesures d'atténuation des risques d'entrave à la vie privée. En outre, le coût et l'efficacité des mesures de protection existantes et proposées calculées au cours et de l'évaluation des vulnérabilités et de la phase des recommandations d'un projet d'EMR prouvent hors de tout doute que les plans, les mesures et les préparatifs de PCA proposés, de même que les mesures recommandées d'atténuation des préoccupations relatives à la vie privée, permettent effectivement l'atteinte de niveaux acceptables de risques résiduels à un coût abordable.

5.3 Évaluation du programme

Tant la PGS que la politique de l'EFVP exigent une surveillance permanente de la conformité afin de déterminer l'efficacité des programmes ministériels relatifs à la PCA, à la vie privée et à la sécurité.[7] Le rapport d'EMR de toutes les installations et de tous les systèmes ou services comprend une analyse objective de l'efficacité des mesures de protection et, par conséquent, des vulnérabilités relatives aux biens et aux services critiques dans un programme de PCA, et des renseignements personnels assujettis à la politique de l'EFVP dans le contexte de l'évaluation. De plus, les risques résiduels inacceptables sont identifiés dans la phase des recommandations,

[7] La section 11 de la PGS exige des ministères qu'ils effectuent une surveillance active de leur programme de sécurité et qu'ils effectuent des vérifications internes, alors que la section 10.14 d) exige des ministères des activités pour surveiller leur niveau de préparation. À la page 12 de la politique, l'EFVP exige des ministères qu'ils évaluent leur degré de conformité à la politique à l'aide de vérifications, d'examens et d'évaluations internes.

qui inclut également des propositions de mesures correctives. Ainsi, le processus analytique d'un projet d'EMR offre un mécanisme idéal d'évaluation de l'efficacité des principaux éléments du programme de PCA et de l'EFVP au minimum, et du programme ministériel de sécurité en général.

6 Conclusion

En résumé, les portées des trois méthodes (ARO, EFVP et EMR) peuvent être très différentes; toutefois, l'objectif sous-jacent de chaque activité, qui vise à favoriser une gestion éclairée des risques, est remarquablement semblable. De plus, on peut établir des parallèles étroits entre le processus interne d'un programme de PCA complet, l'EFVP et une EMR, tel qu'il est illustré dans le tableau B3-1. Compte tenu de la nature complémentaire de ces trois pratiques obligatoires, les interrelations entre les autorités responsables doivent être renforcées, tant au sein des ministères qu'entre eux, pour atteindre les objectifs suivants :

- réaliser une application plus uniforme des mesures de protection complémentaires, donc rentables, pour traiter de manière globale les risques liés à la PCA, à la vie privée et à la sécurité;
- réduire la charge de travail globale en favorisant la réutilisation des éléments de sortie d'un processus comme éléments d'entrée d'un autre, tel qu'il est discuté aux sections 5.5.1 et 5.5.2 plus haut;
- réduire les tensions ou les conflits potentiels entre les mécanismes de confidentialité recommandés dans une EFVP ou une EMR et les mesures relatives à la disponibilité identifiées dans les plans de PCA et les préparatifs ou une autre EMR; et
- attribuer plus efficacement les ressources limitées entre les programmes complémentaires relatifs à la PCA, à la vie privée et à la sécurité.

Appendice B-4 - Tableau détaillé des préjudices

Niveau de préjudice	Préjudices aux personnes		Répercussions financières
	Préjudice physique	**Préjudice psychologique**	
Très élevé	1. Pertes de vie massives	1. Traumatisme psychologique généralisé 2. Agitation civile possible	> 1 milliard $
Élevé	1. Perte de vie possible pour certains 2. Invalidité permanente pour certains 3. Maladie ou blessure grave pour beaucoup 4. Difficultés physiques graves pour beaucoup	1. Profond embarras pour beaucoup 2. Doutes/incertitudes graves pour beaucoup 3. Méfiance généralisée du public 4. Aliénation de vastes groupes	> 10 millions $
Moyen	1. Maladie ou blessure grave pour certains 2. Inconfort grave pour beaucoup 3. Douleurs mineures pour beaucoup	1. Profond embarras pour certains 2. Doutes/incertitudes graves pour certains 3. Inconvénients graves pour beaucoup 4. Embarras mineur pour beaucoup 5. Doutes/incertitudes mineurs pour beaucoup	> 100 000 $
Faible	1. Inconfort grave pour certains 2. Douleurs mineures pour certains 3. Inconfort mineur pour beaucoup	1. Graves inconvénients pour certains 2. Embarras mineur pour certains 3. Doutes/incertitudes mineurs pour certains 4. Inconvénients mineurs pour beaucoup	> 1 000 $
Très faible	1. Négligeable 2. Inconfort mineur pour certains	1. Négligeable 2. Inconvénients mineurs pour certains	< 1 000 $

Nota : La ligne de démarcation entre « beaucoup » et « certains » demeure floue, mais un niveau d'un millier peut se révéler un seuil utile.

1 Instructions

Il faut attribuer une valeur à chaque bien évalué dans le cadre du projet d'EMR en procédant comme suit :

1.1 Étape 1

Déterminez le niveau de ventilation qui convient (groupe, sous groupe, composant ou élément individuel), en vue d'une analyse ultérieure fondée sur les critères de définition de la portée de la section 4 de l'annexe A.

1.2 Étape 2

D'après les niveaux maximums de préjudice qu'on pourrait raisonnablement attendre d'une compromission :

- sélectionnez la valeur de la confidentialité de l'information et d'autres biens, le cas échéant, d'après le préjudice vraisemblable qu'entraînerait leur divulgation non autorisée;
- sélectionnez la valeur de la disponibilité pour tous les membres du personnel (des points de vue intrinsèque et opérationnel), des biens corporels et incorporels et des services, d'après le préjudice vraisemblable qu'entraîneraient leur destruction, leur interruption, leur suppression ou leur utilisation non autorisées;
- sélectionnez la valeur de l'intégrité pour l'information et les processus ou les capteurs qui s'y rapportent d'après le préjudice vraisemblable qu'entraînerait leur modification non autorisée.

1.3 Étape 3

Si le préjudice (physique ou psychologique) subi par les personnes et les répercussions financières découlant d'une seule et même compromission sont différents, inscrivez la valeur la plus élevée dans le tableau d'évaluation des biens/énoncé de sensibilité (appendice B-5).

- Par exemple, si on peut raisonnablement s'attendre à ce que la divulgation non autorisée d'un document n'entraîne pas de préjudice physique, mais un embarras profond pour certains et des pertes financières dépassant 10 millions de dollars, soit des niveaux de préjudice très faible, moyen et élevé, respectivement, il faut attribuer à ce bien la valeur la plus élevée, soit un préjudice élevé (Protégé C, voire même Secret), du point de vue de la confidentialité.
- À l'inverse, si les préjudices découlant de différentes compromissions du même bien sont différents (en d'autres termes, si les valeurs sur les plans de la confidentialité, de la disponibilité et de l'intégrité diffèrent), inscrivez chaque valeur séparément dans le tableau d'évaluation des biens/énoncé de sensibilité
- Par exemple, si la divulgation non autorisée d'un dossier médical peut occasionner un embarras mineur à quelqu'un (préjudice faible), mais que sa perte ou sa destruction non autorisée peuvent entraîner un retard dans le traitement d'une maladie grave, voire même un décès (préjudice élevé), ou que la modification non autorisée des données peut entraîner des erreurs dans le traitement d'une maladie grave et mettre la vie du patient en danger (autre préjudice grave), il faut attribuer une valeur faible à ce bien sur le plan de la confidentialité, mais une valeur élevée sur les plans de la disponibilité et de l'intégrité.

1.4 Étape 4

Si la valeur d'un bien se rapproche de la ligne de démarcation entre deux niveaux, il convient de la baliser au moyen de flèches (↑↓) indiquant si elle se rapproche de l'extrémité supérieure ou de l'extrémité inférieure de la fourchette; elle pourra ainsi faire l'objet d'une analyse subséquente lors de la phase d'évaluation des risques du projet d'EMR. Par exemple, si les répercussions financières prévues d'une compromission sont estimées à 9,8 millions de dollars, soit une valeur moyenne qui se rapproche de la fourchette des valeurs élevées, il convient de l'indiquer en conséquence.

2 Exemples

2.1 Dossier(s) personnel(s)

La nature de l'information figurant dans le dossier et la question de regroupement sont d'importants éléments à prendre en considération au moment de l'évaluation de la confidentialité, de la disponibilité et de l'intégrité des renseignements personnels.

- **Confidentialité.** La divulgation non autorisée d'une seule demande de congé ne causera peut-être aucun préjudice, mais la divulgation accidentelle ou délibérée de l'identité d'un informateur de police peut mettre la vie de celui-ci en danger. Ainsi, dans le premier cas, la valeur de la confidentialité serait très faible (Non classifié), alors que dans le second, elle serait élevée (Protégé C). Si c'est un programme de protection des témoins au complet qui est divulgué, cela pourrait entraîner des pertes de vie massives, de sorte que la valeur de la confidentialité serait très élevée (Très secret). Il faut toutefois savoir que la plupart des dossiers du personnel dans les institutions gouvernementales portent la cote Protégé B, de sorte que leur valeur de confidentialité est moyenne.
- **Disponibilité.** La divulgation non autorisée d'une seule demande de congé pourrait, dans le pire des cas, entraîner une perte financière supérieure à 1 000 $, mais certainement inférieure à 100 000 $, si le relevé de paie de la personne en cause est rajusté en fonction d'un congé d'un mois. Toutefois, si toutes les demandes de congé d'un grand ministère sont détruites, le préjudice pourrait se multiplier par 10 000 ou plus, et les pertes financières possibles dépasseraient 10 millions de dollars. Par conséquent, la valeur d'une seule demande sur le plan de la disponibilité serait faible, mais la valeur de toute la base de données des congés justifierait vraisemblablement une valeur élevée.
- **Intégrité.** Le même raisonnement peut s'appliquer à la valeur de l'intégrité, selon que la compromission vise une seule demande de congé ou toute la base de données des congés; en effet, la modification non autorisée ou l'altération des données pourrait entraîner des pertes financières du même ordre.

2.2 Équipe médicale

Une petite équipe de médecins aurait automatiquement une valeur élevée sur le plan de la disponibilité intrinsèque. Selon les fonctions de chacun, sa valeur sur le plan de la disponibilité opérationnelle pourrait varier considérablement. Par exemple, si les médecins du groupe ne représentent que quelques-uns des nombreux omnipraticiens d'une clinique dans une grande ville, leur absence pourrait causer simplement certains inconvénients et le report de certains rendez-vous avec des patients; en pareil, la valeur du préjudice serait faible ou même très faible, selon le nombre de patients touchés. Mais à l'autre extrême, si les médecins de l'équipe sont les seuls en mesure de limiter une pandémie de grande envergure et donc d'empêcher des pertes de vie massives, leur valeur sur le plan de la disponibilité opérationnelle serait très élevée. Même si l'équipe médicale a sans aucun doute accès à des informations confidentielles et à d'autres biens de nature délicate, aucune valeur ne serait normalement attribuée à ses membres sur les plans de la confidentialité ou de l'intégrité.

Page intentionnellement laissée en blanc

Appendice B-5 - Tableau d'évaluation des biens / Énoncé de sensibilité

Classe	Catégorie	Groupe	Sous-groupe	Composant ou élément individuel	Valeurs des biens				
					C	D[1]		I	$
						In	Op		
Personnes									
Biens corporels	Information								
	Matériel informatique								
	Logiciels								
	Processus								
	Installations								
Services									
Biens incorporels									

Légende

C – Valeur de confidentialité. D – Valeur de disponibilité.
In – Valeur de disponibilité intrinsèque pour le personnel. Op – Valeur de disponibilité opérationnelle pour le personnel. I – Valeur d'intégrité. $ - Coût de remplacement.

INSTRUCTIONS

[1] La colonne de la disponibilité est divisée en deux, soit disponibilité intrinsèque (In) et disponibilité opérationnelle (Op).

Étape 1. Entrez tous les biens visés par le projet d'EMR au niveau de ventilation qui convient (groupe, sous-groupe, composant ou élément individuel), à partir de la liste des biens de l'appendice B-2.

Étape 2. D'après les niveaux maximums de préjudice qu'on pourrait raisonnablement attendre d'une compromission de leur confidentialité (C), de leur disponibilité (D) ou de leur intégrité (I), entrez les valeurs pertinentes des biens qui ont été déterminées conformément au tableau détaillé des préjudices de l'appendice B-4, sur une échelle allant de Très faible (TF) à Très élevé (TE). Si c'est la sécurité personnelle d'un individu qui est en cause, attribuez-lui une valeur intrinsèque (In) et une valeur opérationnelle (Op) dans la colonne de la disponibilité.

Étape 3. Si une valeur se rapproche de la ligne de démarcation entre deux niveaux, utilisez des flèches pour indiquer si elle se rapproche de l'extrémité supérieure (↑) ou de l'extrémité inférieure (↓) de la fourchette.

Annexe C - Phase d'évaluation des menaces

1 Introduction

1.1 Généralités

La troisième phase d'un projet d'EMR, l'évaluation des menaces, compte quatre processus successifs et un résultat important, soit :

- **Identification des menaces** – produire au niveau de détail approprié la liste de toutes les menaces susceptibles d'avoir une incidence sur les biens prévus dans la portée de l'évaluation.
- **Évaluation de la probabilité** – évaluer la probabilité que chaque menace se matérialise;
- **Évaluation de la gravité** – déterminer l'incidence potentielle de chaque menace.
- **Évaluation des menaces** – attribuer à chaque menace des niveaux de menace, de très faible à très élevée, fondés sur des paramètres communs de probabilité et de gravité.
- **Tableau priorisé des menaces** – produire une liste exhaustive des menaces, classées en ordre de la plus grave à la moins grave.

1.2 But

Le but de cette annexe est de décrire les quatre processus et le résultat unique de la phase d'évaluation des menaces d'un projet d'EMR.

2 Identification des menaces

2.1 Définition du terme « menace »

La PGS définit une menace comme « tout événement ou acte éventuel, délibéré ou accidentel, qui pourrait porter préjudice aux employés ou aux biens. »[1] Bien que très convenable, cette définition peut être élargie dans deux directions. Dans un premier temps, on doit tenir compte dans chaque évaluation d'une autre grande catégorie de menaces, à savoir les risques naturels, puisqu'ils peuvent avoir de très graves conséquences, notamment au plan de la disponibilité. Deuxièmement, tout préjudice causé à des biens ou des employés aura probablement une incidence sur la prestation de services. On doit donc élargir la définition pour tenir compte de cette éventualité.

> ***Menace*** (*threat*) – tout événement ou acte éventuel, délibéré ou accidentel, ou risque naturel qui pourrait porter préjudice aux employés ou aux biens et ainsi avoir une incidence négative sur la prestation de services.
>
> Définition élargie de la PGS

[1] Appendice B de la PGS, Glossaire.

2.2 Classes de menace

2.2.1 Généralités

Tel que l'indique la définition élargie de la PGS, les menaces peuvent être catégorisées selon leurs causes réelles, soit humaines ou naturelles (forces de la nature). Les causes humaines peuvent être subdivisées en menaces délibérées (événements planifiés) et accidents (événements non planifiés). Chacune de ces trois grandes classes possèdent des caractéristiques variées dont on doit tenir compte au cours de la phase d'évaluation des menaces d'un projet d'EMR.

2.2.2 Menaces délibérées

Par définition, toutes les menaces délibérées sont le fait d'êtres humains et présument une certaine planification ou préméditation. À vrai dire, certains commettent des actes spontanés sous l'impulsion du moment, sans beaucoup réfléchir aux conséquences. Malgré tout, même ce type de menace exige une prise de décision consciente concernant la mesure à prendre. Puisque les menaces délibérées sont souvent menées en secret, elles peuvent être plus difficiles à identifier, évaluer et prévoir que les accidents et les risques naturels. De plus, la sélection de contre-mesures appropriées pour atténuer les vulnérabilités connexes peut s'avérer beaucoup plus complexe compte tenu qu'un adversaire intelligent analysera fréquemment la situation et prendra les moyens pour contourner les mesures de protection visibles tout en recourant à un subterfuge pour éviter d'être détecté. Ce genre de menace peut entraîner tous les types de compromission de la confidentialité, de la disponibilité et de l'intégrité (divulgation, destruction, élimination, modification, interruption ou utilisation non autorisées de biens). Les incidences potentielles de ces menaces peuvent varier considérablement, du vol presque innocent de matériel de bureau aux dommages considérables causés par une attaque terroriste majeure.

2.2.3 Menaces accidentelles

Tous les accidents sont le fait d'erreurs humaines sous une forme ou une autre. Un employé ou toute autre personne qui n'a reçu aucun formation ou qui est mal informée peut commettre diverses erreurs, allant de l'altération par inadvertance des données ou de la divulgation d'information par suite d'une erreur d'exploitation causée par un défaut de conception jusqu'aux défaillances mécaniques et même structurales. Comme dans le cas des menaces délibérées, les incidences possibles des accidents incluent toutes les formes de compromission, incluant des incidences possibles sur la confidentialité, la disponibilité et l'intégrité. Des accidents, tels un café renversé ou une lettre pleine de fautes, sont fréquemment sans conséquences, alors que les effets négatifs de certains incidents, tel un déversement toxique majeur ou une erreur de pilotage à bord d'un gros avion commercial, peuvent être vraiment catastrophiques.

2.2.4 Risques naturels

Bien que les risques naturels soient aussi variés que les accidents et les menaces délibérées, leurs conséquences sont généralement plus ciblées. Essentiellement, les forces de la nature sont rarement à l'origine d'une divulgation ou d'une modification non autorisée, ou de compromissions de la confidentialité et de l'intégrité. Évidemment, il y a quelques exceptions : une tornade peut détruire un immeuble et disséminer des documents sensibles dans la nature, ou la foudre peut créer une surcharge de courant susceptible d'altérer des fichiers de données électroniques. Néanmoins, les risques naturels ont généralement pour conséquences des compromissions variées de la disponibilité, telles des blessures aux personnes, la destruction

d'autres biens et l'interruption de services. Des phénomènes naturels susceptibles de causer des dommages surviennent régulièrement, mais des désastres graves sont beaucoup moins fréquents.

2.2.5 Modèle de menace

La figure C-1 illustre les relations entre les trois grandes classes de menace dans un modèle général de menace.

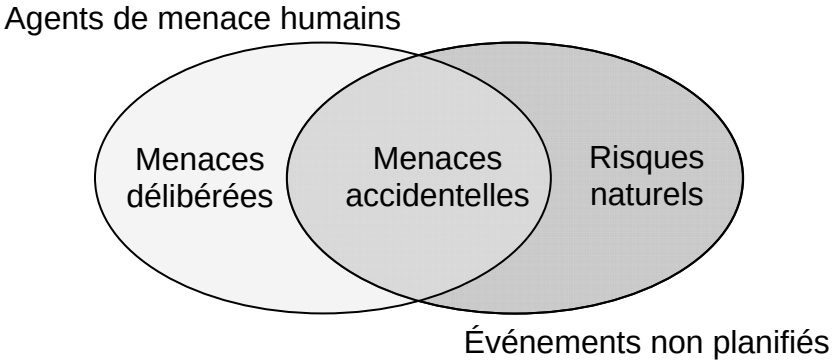

Figure C-1 : Modèle général de menace

2.3 Sources des données sur les menaces

Plusieurs analystes de risques perçoivent l'évaluation des menaces comme la phase la plus stimulante d'un projet d'EMR compte tenu de la rareté perçue de données pertinentes ou de renseignements actuels. Toutefois, rien n'est plus faux, puisqu'il existe des masses de renseignements que l'on peut se procurer facilement auprès d'une variété de sources fiables. Les gestionnaires de programme et les employés peuvent être conscients des problèmes imminents, plus particulièrement pour ce qui touche certaines menaces accidentelles et préoccupations immédiates; toutefois, les autorités ministérielles chargées de la sécurité, les gestionnaires d'installations et les administrateurs de systèmes sont plus susceptibles d'avoir une perception plus large des niveaux de menace actuels. Les rapports sur les incidents, les évaluations de renseignements et les vérifications internes s'avèrent souvent des sources utiles d'information sur les menaces. Les médias, plus particulièrement la presse locale et nationale, peuvent fournir des renseignements valables, de même qu'une vaste gamme de revues professionnelles et de sites Web connexes qui peuvent aussi être utiles. Ces intervenants, ainsi que d'autres sources, figurent dans la liste à l'appendice C-1.

2.4 Techniques de collecte des données

Bien que les données sur les menaces soient facilement repérables, il n'existe pas de dépôt central pour cette information. Le vrai dilemme pour les spécialistes de la sécurité est donc de pouvoir collecter, regrouper et analyser en temps opportun des renseignements largement dispersés pour répondre aux besoins de chaque projet d'EMR. Sans un programme permanent de tenue à jour d'un inventaire central des menaces, trop d'analystes de risques doivent repartir à zéro à chaque évaluation, ce qui a pour effet d'allonger le travail, d'augmenter les coûts et de

donner lieu à de dangereuses méprises dans les cas où des menaces importantes ne sont pas prises en compte.

Pour éviter ces pièges, les ministères peuvent envisager deux options différentes pour la collecte, le regroupement et l'analyse de données sur les menaces. Les plus petits organismes qui effectuent des projets d'EMR relativement peu fréquemment, trouveront probablement plus rentable d'embaucher un conseiller possédant les compétences appropriées et de lui confier le soin de compiler les évaluations des menaces requises. D'autre part, les plus grandes organisations, qui ont des besoins périodiques réguliers, jugeront plus efficace d'établir une cellule spécialisée d'analystes des menaces chargée d'élaborer et de tenir à jour une base de données permanente des menaces à l'appui de l'ensemble des projets d'EMR.

2.5 Liste des menaces

2.5.1 Structure

La liste des menaces à l'appendice C-2 est présentée sous forme de tableau hiérarchique dont la structure s'inspire de celle de la liste des biens de l'appendice B-2. À partir du plus haut niveau des trois grandes classes de menaces définies à la section 2.2, la liste se développe et tient compte des activités de menace plus détaillées, des catégories d'agents de menace, des agents de menace, des incidents et, le cas échéant, des scénarios de menace spécifiques permettant une analyse de plus en plus granulaire. Chacun des niveaux subordonnés sont définis ci-dessous et la structure elle-même est illustrée dans la figure C-2.

- **Activité de menace.** Groupe générique de menaces ayant des conséquences ou des résultats communs, dont le but est de faciliter la collecte des données aux ministères ou organismes gouvernementaux responsables.
- **Catégorie d'agent de menace.** Subdivision d'une activité de menace, dont le but est de mettre l'accent sur les menaces délibérées dont la motivation est la même, ou sur les menaces accidentelles et les risques naturels dont les facteurs déterminants sont similaires.
- **Agent de menace.** Organisation, individu ou type d'individu identifiables et susceptibles d'être à l'origine de menaces délibérées, ou type spécifique d'accident ou de risque naturel.
- **Incident.** Incident réel au cours duquel un agent de menace exploite une vulnérabilité susceptible d'avoir une incidence négative sur un bien de valeur.
- **Scénario de menace.** Description chronologique et fonctionnelle détaillée d'un incident réel ou hypothétique, dont le but est de faciliter de manière générale l'analyse du risque et plus particulièrement l'identification des mesures de protection appropriées.

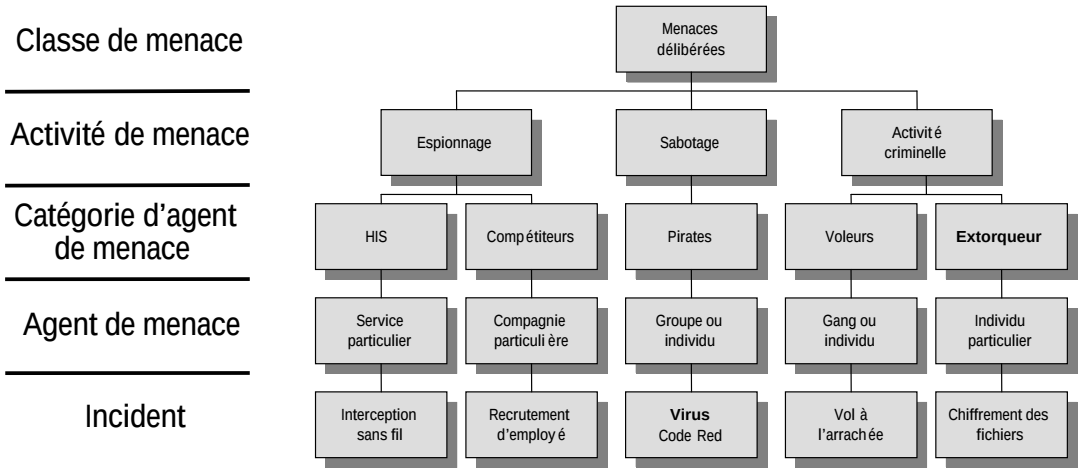

Figure C-2 : Exemple de segment de la structure hiérarchique de la liste des menaces[2]

2.5.2 Avantages

Comme la liste des biens, la liste à structure hiérarchique des menaces offre plusieurs avantages importants lors de l'exécution d'un projet d'EMR :

- **Cohérence.** L'utilisation de structures et de définitions de données communes pour l'identification des menaces facilite les communications au sein des projets d'EMR et entre ceux-ci, et permet d'obtenir des résultats cohérents que peuvent reproduire différents spécialistes qui évaluent des menaces identiques ou similaires. Elle favorise également l'interopérabilité et le partage de données sur les menaces entre les organisations.
- **Exhaustivité.** L'utilisation d'une liste détaillée pour guider les équipes d'EMR rend moins probable l'omission de menaces importantes.
- **Flexibilité et extensibilité.** L'aspect le plus important est la structure hiérarchique de la liste des menaces qui permet des analyses à différents niveaux de détails conformes au champ d'application de l'évaluation et à l'environnement de risque réel. Essentiellement, cette caractéristique permet de regrouper et d'évaluer à un niveau supérieur des menaces moins sérieuses pour des biens de moindre valeur, tout en permettant d'examiner au niveau de l'agent de menace ou de l'incident les menaces qui représentent de plus grands risques et, ainsi, d'obtenir une plus grande précision. Dans le même ordre d'idées, on peut omettre complètement des branches entières de la structure arborescente dans le cas où une activité de menace ou une catégorie d'agent de menace particulière déborde de la portée de l'évaluation. Ainsi, les équipes d'EMR peuvent cibler leurs efforts et se concentrer sur ce qui est vraiment important.
- **Documentation à jour.** On peut facilement tenir la liste des menaces à jour au fur et à mesure que l'on identifie de nouvelles menaces. De plus, en raison du

[2] L'abréviation HIS signifie *Hostile Intelligence Service* ou Service de renseignement ennemi.

regroupement logique de menaces similaires, il est beaucoup plus simple de catégoriser les problèmes, nouveaux ou naissants.

2.5.3 Mise en garde

Encore une fois, comme c'est le cas pour la liste des biens, on doit utiliser la liste des menaces avec prudence. Cette liste n'est pas complète, et ne peut l'être, puisque de nouvelles menaces, plus particulièrement au niveau de l'analyse des incidents, se manifestent régulièrement en raison, entre autres, des technologies et des capacités des agents de menace en constante évolution. **On doit donc utiliser l'appendice C-2 comme un guide ou un aide-mémoire pour aider à organiser et structurer la collecte et le regroupement des données pertinentes sur les menaces, plutôt que comme une liste de vérification à suivre aveuglément.**

2.6 Activités de menace

2.6.1 Généralités

Les trois grandes classes de menace, soit les menaces délibérées, les menaces accidentelles et les risques naturels, incluent plusieurs activités différentes de menace susceptibles de compromettre des biens, tant corporels qu'incorporels, de causer des préjudices aux employés et de perturber la prestation de services.

2.6.2 Activités de menace délibérées

Les activités de menace liées à la classe des menaces délibérées incluent les suivantes :

- **Guerre.** Tant les guerres civiles qu'internationales ou les révolutions peuvent s'avérer extrêmement destructives et susceptibles de compromettre presque tous les biens imaginables de toutes les manières possibles. À ce titre, l'ampleur même d'une guerre peut compliquer considérablement toute évaluation connexe des menaces. C'est pourquoi la méthodologie harmonisée d'EMR a tendance à mettre l'accent sur les menaces et les risques en temps de paix, bien que le processus analytique n'en soit pas moins applicable à des situations de conflits armés.
- **Espionnage.** La collecte d'information par des moyens secrets ou clandestins ne se limite pas aux activités des services de renseignement ennemis. Dans la sphère économique, par exemple, certains compétiteurs se tournent vers l'espionnage industriel pour tirer un avantage concurrentiel. De nombreux pirates, à la fois des individus et des groupes organisés, posent des problèmes similaires lorsqu'ils tentent d'accéder sans autorisation à des ordinateurs et à des fichiers de données, parfois par simple curiosité, mais plus souvent avec des intentions criminelles et malveillantes. D'autres tentatives de collecte d'information, même effectuées subrepticement, peuvent être tout à fait légales. Par exemple, le journalisme d'enquête et la veille concurrentielle recourent à des méthodes tout à fait éthiques qui consistent à recueillir et à analyser des données de sources ouvertes pour acquérir des perspectives sur une entreprise et tirer un avantage concurrentiel. Dans chaque cas, la divulgation non autorisée, préoccupation liée à la nature confidentielle de l'information, est la principale conséquence de l'espionnage et des activités connexes de collecte de données; toutefois, le vol de matériel sensible à des fins d'examen et, à l'occasion, de rétroingénierie peut également poser un problème au plan de la disponibilité.

- **Sabotage.** Le *Code criminel* définit de manière explicite le sabotage comme « un acte ou une omission qui, selon le cas a) diminue l'efficacité ou gêne le fonctionnement de tout navire, véhicule, aéronef, machine, appareil ou autre chose; ou b) fait perdre, endommager ou détruire des biens, quel qu'en soit le propriétaire »[3], si l'on s'en sert à des fins préjudiciables à la sécurité ou à la défense du Canada ou de toute force alliée au Canada. Bien que cette définition convienne dans un contexte national, d'autres intérêts et organismes peuvent être la cible d'attaques similaires. Par exemple, des employés mécontents, des activistes individuels, des groupes radicaux et même des concurrents commerciaux ont endommagé du matériel et interrompu des services pour leur bénéfice personnel ou en raison de faux idéaux. Dans chaque cas, les principales conséquences sont la destruction de biens corporels, associée à une interruption de service, deux conséquences qui ont une incidence sur la disponibilité.
- **Subversion.** La subversion diffère des autres activités de menace en ce qu'elle cible généralement les biens incorporels, telle la confiance du public et le moral des employés. Au sommet du spectre, la *Loi sur le Service canadien du renseignement de sécurité (SCRS)* définit à la fois la subversion d'État, soit « les activités influencées par l'étranger qui touchent le Canada ou s'y déroulent et sont préjudiciables à ses intérêts, et qui sont d'une nature clandestine ou trompeuse ou comportent des menaces envers quiconque » et la subversion domestique, soit « les activités qui, par des actions cachées et illicites, visent à saper le régime de gouvernement constitutionnellement établi au Canada ou dont le but immédiat ou ultime est sa destruction ou son renversement, par la violence ».[4] Évidemment, cette loi prévoit également des dispositions explicites pour protéger les activités licites de défense d'une cause, de protestation ou de manifestation d'un désaccord. Néanmoins, même les activités tout à fait licites, tel le piquetage légal et la distribution de tracts, peuvent justifier une analyse dans un projet d'EMR pour aider à atténuer l'incidence sur la productivité, l'opinion publique et les attentes des employés.
- **Terrorisme.** Comme c'est le cas pour la subversion, le terrorisme est défini dans la *Loi sur le SCRS* comme suit : « activités qui touchent le Canada ou s'y déroulent et visent à favoriser l'usage de la violence grave ou de menaces de violence contre des personnes ou des biens dans le but d'atteindre un objectif politique, religieux ou idéologique au Canada ou dans un État étranger ».[5] Évidemment, les conséquences des deux types de terrorisme, domestique et international, peuvent inclure des préjudices aux personnes, la destruction de biens de valeur et l'interruption de services importants, en plus d'avoir des incidences potentiellement graves sur la disponibilité.
- **Actes criminels.** Le *Code criminel du Canada* et les lois connexes, telle la *Loi sur les stupéfiants*, établissent un fondement légal pour l'application des lois tout en définissant un éventail d'actes illicites qui constituent des menaces pour l'ordre public, l'administration des lois et de la justice, la moralité publique, les simples

[3] *Le Code criminel*. R.S., 1985, c. c-46, a.52(2).
[4] *Loi sur le Service canadien du renseignement de sécurité*. 1984, c. 21, a. 2.
[5] *Ibid.*

citoyens, les fonctionnaires, la propriété, les devises, les marchés et le commerce entre autres biens corporels et incorporels de valeur. Compte tenu de la variété des actes criminels, leurs conséquences potentielles incluent tous les types possibles de compromission qui ont une incidence sur la confidentialité, l'intégrité et la disponibilité, ainsi que sur le coût de remplacement. Certes, la distinction entre les actes criminels et les autres activités de menace délibérée mentionnées précédemment est quelque peu artificielle puisque ces dernières impliquent presque invariablement un ou plusieurs actes criminels. Par exemple, certains actes d'espionnage peuvent être associés à de la trahison [paragr. 46(2)] et quelques uns incluent l'interception de communications privées [paragr. 184(1)] ou l'utilisation non autorisée d'un ordinateur [paragr. 342(1)]; tel qu'il a été souligné précédemment, le sabotage [paragr. 52(2)] est déjà un acte criminel; les activités subversives peuvent inclure la sédition [paragr. 59(1)], l'attroupement illégal [paragr. 63(1)], la diffusion de fausses nouvelles [paragr. 181], le méfait [paragr. 430(1)] ou, dans des cas extrêmes, l'émeute [paragr. 64]; et, finalement, toutes les attaques terroristes impliquent également des actes criminels, tels le meurtre [paragr. 229], l'utilisation d'explosifs [paragr. 81(1)] ou l'enlèvement [paragr. 279(1)]. Donc, les activités de menace délibérée indiquées dans la liste de l'appendice C-2 ne sont pas toujours mutuellement exclusives. Toutefois, plutôt que de comprimer ou de combiner la liste, il est toujours utile d'établir une distinction entre les sept différents regroupements pour faciliter la collecte, le regroupement et l'analyse des données, plus particulièrement dans le cas où différents organismes ont comme principale responsabilité celle d'enquêter sur certaines activités.

- **Autres activités de menace délibérées.** Tel qu'il est indiqué ci-dessus, on remarque un certain degré d'activité criminelle sous-jacent à la majorité des menaces délibérées; toutefois, il existe des exceptions dignes de mention. À titre d'exemple, l'absentéisme excessif, la navigation à des fins personnelles sur le Web, le courrier électronique non sollicité (pourriel) et les grèves légales peuvent avoir de sérieuses conséquences; toutefois, ce sont des activités licites au Canada, malgré leur incidence négative sur la disponibilité des employés, des biens et des services.

2.6.3 Activités de menace accidentelles

Tous les accidents, à un stade ou à un autre, sont dus à des erreurs humaines commises directement ou indirectement. Les facteurs déterminants de ces incidents incluent une hâte intempestive, le non respect de directives ou de procédures opérationnelles standard, une formation déficiente, une piètre qualité d'exécution, un entretien ménager qui laisse à désirer, des calculs erronés, des mesures de réduction de coûts, le surmenage ou la fatigue. Les conséquences des accidents peuvent inclure toutes les formes de compromission de la confidentialité, de la disponibilité et de l'intégrité. L'incidence de certaines menaces liées à des événements accidentels, telles les fautes d'orthographe dans un rapport ou des fournitures de bureau égarées, peut être anodine; par contre, les effets d'autres incidents, telle la panne majeure de courant du mois d'août 2003 ou la fusion du cœur du réacteur de Chernobyl, peuvent être extrêmement graves. Les différentes activités de menace de la classe des menaces accidentelles incluent les suivantes :

- **Accidents au bureau.** Variété d'erreurs qui ont généralement une incidence sur la confidentialité (correspondance acheminée incorrectement ou catégorisation erronée des données) ou la disponibilité (fichiers de données supprimés à la hâte ou ordinateur bloc-notes échappé); elles n'ont souvent que des conséquences mineures mais, à l'occasion, elles peuvent avoir des résultats plus graves, telles des blessures personnelles ou la mort.
- **Altération des données.** Préoccupation liée à l'intégrité et qui concerne les erreurs de saisie de données et les autres erreurs commises au cours de la collecte, du traitement et de la dissémination de l'information.
- **Perte de biens.** Préoccupation liée à la disponibilité qui concerne les biens corporels, tel l'équipement de bureau ou des titres négociables, égarés par inadvertance et qui ne peuvent être utilisés aux fins pour lesquelles ils ont été conçus.
- **Défaillances mécaniques.** Les défauts de conception, la maintenance inappropriée et les erreurs d'opérateur, qui peuvent contribuer au mauvais fonctionnement de l'équipement, posent normalement un problème au niveau de la disponibilité et donnent lieu à une gamme de conséquences, de négligeables (un crayon brisé) à catastrophiques (un déraillement ferroviaire majeur).
- **Erreurs logicielles.** Les erreurs de codage, l'intégration imparfaite du logiciel et les autres erreurs d'installation peuvent compromettre tant la confidentialité que l'intégrité; toutefois, les incidences les plus communes sont des problèmes de disponibilité dus au mauvais fonctionnement des systèmes concernés.
- **Défectuosités matérielles.** Comme l'équipement mécanique, le matériel informatique peut mal fonctionner en raison de défauts de conception, d'une maintenance inappropriée et d'erreurs d'opérateur, et donner lieu à une gamme de conséquences, de presque négligeables (un moniteur grillé) à extrêmement graves (défaillance de puces multiples de l'ensemble avionique d'un jumbo jet). Bien que la plupart des incidents concernent la disponibilité, certains se répercutent au plan de l'intégrité (coprocesseurs mathématiques défaillants).
- **Défaillances de structure.** Événements relativement rares mais potentiellement graves dus à des erreurs de calcul d'ingénierie, des erreurs de construction ou des problèmes de maintenance et qui peuvent mener à un effondrement partiel ou total d'immeubles et autres structures, problèmes souvent aggravés par des risques naturels concurrents telle de la pluie verglaçante ou une abondante chute de neige.
- **Incendies.** Problème lié à la disponibilité et ayant des conséquences potentiellement graves pour les employés, les biens corporels et, par conséquent, la prestation de services; ce type de problème est habituellement associé à de l'insouciance, un entretien ménager qui laisse à désirer, un entretien inapproprié ou une erreur d'opérateur.
- **Accidents routiers.** Généralement causés par une erreur du conducteur, ces incidents sont souvent aggravés par des conditions météorologiques ou routières défavorables mais peuvent être dus, à l'occasion, à des erreurs de conception ou à un entretien défaillant; ils ont des conséquences potentiellement graves pour la disponibilité des véhicules, de leurs occupants et des autres biens ambiants.
- **Accidents industriels.** Ces incidents, qui font l'objet d'un vaste ensemble de préoccupations au plan de la disponibilité, sont habituellement attribués à des erreurs

d'opérateur et, moins fréquemment, à des bris d'équipement; leurs conséquences, de nulles (légers retards) à extrêmement graves (déversements toxiques majeurs), ont une incidence sur les employés et les autres personnes, sur les biens corporels et, par conséquent, sur la prestation des services.

- **Accidents nucléaires.** Événements relativement rares qui ont des conséquences potentiellement graves sur la disponibilité des personnes et des biens corporels dans les zones contaminées ainsi que sur la disponibilité des services offerts et, par conséquent, sur celle des biens incorporels, telle la confiance du public.

2.6.4 Activités de menace liées aux risques naturels

Plusieurs forces différentes de la nature peuvent être à l'origine d'une grande variété d'incidents ayant des conséquences variées sur la disponibilité. Les activités de la classe des menaces liées aux risques naturels incluent les suivantes :

- **Maladies.** Les maladies qui affectent les personnes ou les plantes et les animaux dont ils dépendent sont généralement causées par des micro-organismes ou des défauts génétiques et leurs incidences vont du léger inconfort (léger rhume) à des événements catastrophiques (pandémie de grippe mondiale).
- **Mouvements de terrain.** Certains mouvements, telle l'érosion et le tassement de terrain, ont pour effet de miner les structures relativement lentement sur une longue période, alors que d'autres, tels les glissements de terrain, les éruptions volcaniques et les tremblements de terre, peuvent causer, très subitement et avec peu d'avertissement, des dommages à la fois locaux et occasionnellement étendus.
- **Inondations.** Les précipitations saisonnières, le ruissellement, les tempêtes violentes, les marées hautes et, beaucoup plus rarement, les tsunamis peuvent être à l'origine d'une crue parfois très rapide des eaux et causer des préjudices aux personnes et aux biens corporels en plus d'interrompre parfois les services sur un vaste territoire pendant de longues périodes.
- **Environnement.** Les personnes et les biens corporels peuvent subir des préjudices résultant d'une variété de facteurs environnementaux, telles des particules en suspension dans l'air (tant la poussière que le pollen), des températures extrêmes (chaudes et froides) et le rayonnement ambiant (radon); d'autres facteurs, telles l'humidité, les tempêtes géomagnétiques et l'électricité statique, ont généralement des incidences plus sévères sur les biens corporels.
- **Tempêtes violentes.** Des vents violents très ciblés (tornades) ou largement dispersés sur de grandes étendues (ouragans et typhons) peuvent causer des blessures aux personnes, des dommages aux biens corporels et des interruptions de service, alors que d'autres effets secondaires de violentes tempêtes, telle la foudre, de fortes précipitations, de la pluie verglaçante, d'abondantes chutes de neige et des tempêtes de grêle, peuvent également causer des dommages sérieux.
- **Plantes et animaux.** Les plantes nocives peuvent déplacer des variétés de plantes indigènes et produire des effets écologiques à long terme, alors que les plantes toxiques peuvent causer des préjudices immédiats aux personnes et autres créatures vivantes. Il arrive que des humains soient attaqués directement par différents animaux, y compris des ours, des requins et divers insectes ou reptiles vénéneux;

d'autres incidents sont liés à des collisions (avec un chevreuil, un orignal ou des oiseaux), des infestations d'insectes (fourmis, coquerelles et termites), dont certains peuvent être des vecteurs de maladies graves (tiques qui transmettent la maladie de Lyme), et même causer des pannes de courant dans le cas d'isolants rongés, sources de courts-circuits.

2.7 Menaces directes et indirectes

2.7.1 Définitions

Les interactions des menaces avec les biens de valeur vont des événements très simples à des scénarios extrêmement complexes. Les **menaces directes**, où un seul agent de menace exploite une vulnérabilité pour compromettre un bien, sont généralement simples et faciles à analyser. Par contre, la suite d'événements peut s'avérer beaucoup plus complexe dans le cas des **menaces indirectes**, où un ou plusieurs agents de menace œuvrent individuellement ou collectivement pour exploiter des vulnérabilités successives et ultimement compromettre un bien quelconque. La figure C-3 illustre à la fois les menaces directes et les menaces indirectes simples.

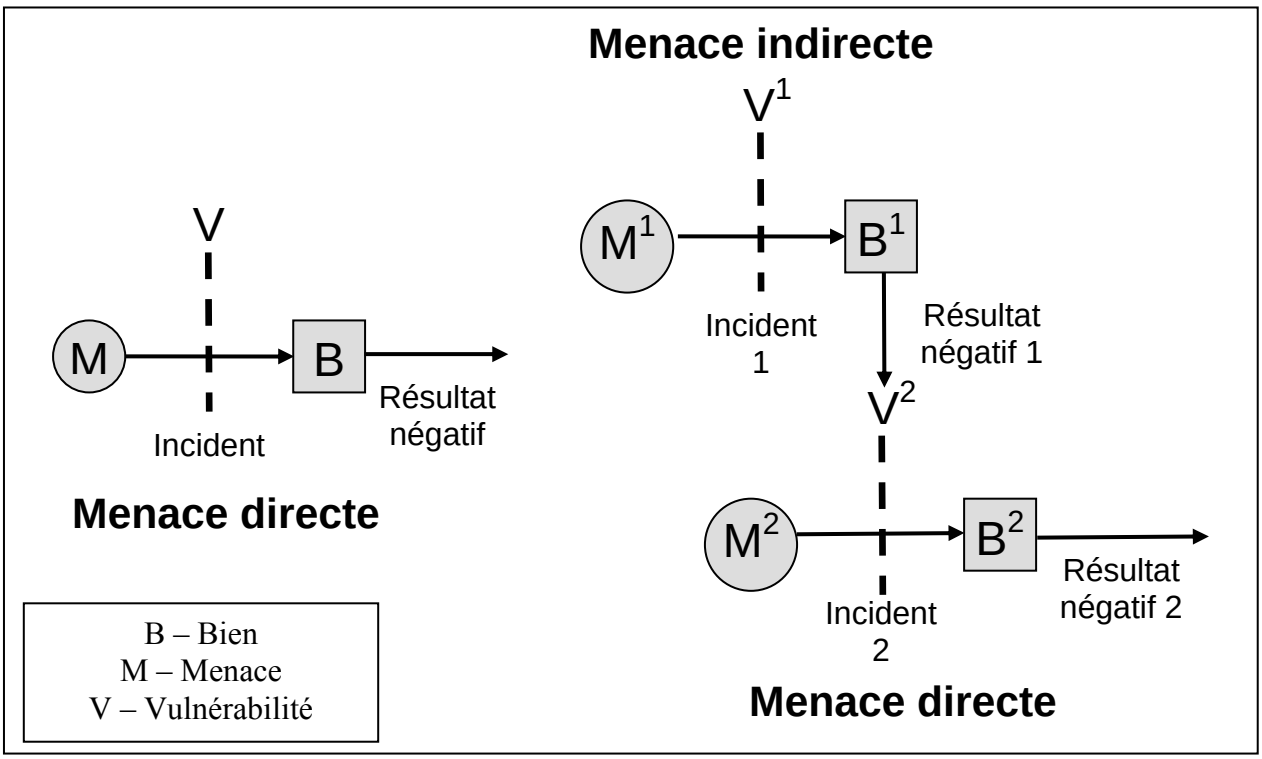

Figure C-3 : Menaces directes et indirectes

2.7.2 Conséquences pratiques

Bien qu'il soit possible de préparer des scénarios d'attaque alambiqués durant la phase d'évaluation des menaces d'un projet d'EMR, cet effort n'est pas justifié pour deux raisons principales. Dans un premier temps, chacune des étapes d'une suite complexe d'événements a une faible probabilité de se produire; puisque ces étapes sont cumulatives, la probabilité finale de réussite diminue très rapidement avec chaque élément intermédiaire d'une menace complexe. Deuxièmement, les mesures de protection sélectionnées durant la phase de recommandation d'un projet d'EMR pour atténuer les menaces directes et les menaces indirectes simples permettent souvent de contrer également des menaces plus compliquées. Les analystes d'EMR, au cours d'une évaluation formelle, doivent donc mettre l'accent sur les menaces directes et les menaces indirectes plus évidentes plutôt que de consacrer inutilement du temps à des spéculations très audacieuses.

2.8 Paramètres des menaces

2.8.1 Exigences de la PGS

Au plus haut niveau d'abstraction, l'article 10.7 de la PGS exige des ministères du gouvernement qu'ils identifient les menaces envers les employés et les biens, et évaluent la **probabilité** qu'elles se concrétisent et leur **incidence**.

2.8.2 Paramètres harmonisés de l'EMR

Ces deux dimensions, probabilité et incidence, sont à la base d'une mesure objective qui permet une analyse comparative. Effectivement, des incidents très probables ou simplement possibles contribuent davantage au risque que les autres possibilités éloignées. Dans le même ordre d'idées, l'incidence ou l'étendue de la compromission résultante augmente au fur et à mesure que s'accroît l'ampleur ou la gravité d'un incident. La méthodologie harmonisée d'EMR s'articule sur ces concepts pour établir des paramètres quantitatifs qui permettent une évaluation objective des menaces.

3 Évaluation de la probabilité

3.1 Généralités

À l'occasion, le renseignement de situation peut prédire certaines menaces délibérées et divers détecteurs, donner des avertissements sur certains accidents ou risques naturels. Malheureusement, il est possible que de tels indicateurs ne soient pas disponibles en plus de ne pas être toujours fiables. De plus, les projections qu'ils permettent visent souvent le court terme, offrant peu de possibilité pour les évaluations de risques à long terme et la sélection de mesures de protection appropriées. Compte tenu de ces contraintes, on a normalement besoin d'autres paramètres pour évaluer la probabilité des menaces prévues dans le champ d'application d'un projet d'EMR.

3.2 Fréquence

Intuitivement, l'expérience récente fournit probablement le meilleur indicateur des tendances futures. Essentiellement, les incidents qui se sont produits plus fréquemment par le passé sont plus susceptibles de survenir dans le futur, sauf si un facteur quelconque entre en jeu et modifie les modèles sous-jacents. Par exemple, si le vol s'est avéré un problème persistent au cours des derniers six mois ou plus, il est probable qu'il continuera d'être une préoccupation sérieuse dans un avenir prévisible. D'autres menaces, tels les tremblements de terre catastrophiques, sont extrêmement rares dans la plupart des endroits et continueront probablement de l'être. Donc, aux fins d'analyse, la probabilité d'activités de menace ou d'événements pertinents, notamment ceux qui se produisent dans l'environnement immédiat et qui ont une incidence sur les sous-groupes de biens prévus dans le champ d'application de l'évaluation, doit être dérivée des sources inclues dans la liste de l'appendice C-1, et on doit lui attribuer un des quatre niveaux de gravité du tableau C-1, selon la fréquence passée des occurrences, de quotidienne à des intervalles de plus de 10 000 jours (soit environ 30 ans ou plus entre les incidents).

3.3 Autres considérations

3.3.1 Intentions des agents de menace

La probabilité des menaces délibérées peut être plus volatile que celle des accidents et des risques naturels puisque les intentions des agents de menace peuvent changer avec peu d'avertissement. Par exemple, des groupes de terroristes, qui par le passé avaient limité leurs attaques à une région, ont à l'occasion porté leur attention vers d'autres cibles ailleurs dans le monde. Il ne suffit donc pas de fonder la probabilité d'un incident délibéré uniquement sur l'expérience passée dans le cas de sous-groupes de biens semblables dans le périmètre immédiat du projet d'EMR. Les incidents dans d'autres endroits et ceux qui ont une incidence sur d'autres sous-groupes de biens peuvent également fournir des indicateurs importants.

3.3.2 Endroit

Évidemment, la probabilité de plusieurs menaces délibérées peut varier d'un endroit à l'autre. Par exemple, les vols à main armée se produisent plus fréquemment dans les grandes zones métropolitaines que dans les petits centres ruraux. Il y a presque inévitablement certaines exceptions où les niveaux de menace demeurent relativement constants d'un site à l'autre. Par exemple, les menaces à l'égard de biens de TI connectés à Internet sont généralement les mêmes que pour des cibles similaires, quel que soit l'endroit où elles se trouvent puisque les systèmes sont tous potentiellement accessibles de n'importe où sur la planète. Dans la plupart des cas, toutefois, les incidents qui se sont produits dans le périmètre immédiat sont plus susceptibles de causer des dommages futurs que ceux qui se sont produits ailleurs à une certaine distance. Cela dit, si une menace délibérée s'est matérialisée dans un autre endroit, il existe une certaine possibilité qu'elle ait ultérieurement une incidence sur des biens prévus dans le champ d'application de l'évaluation puisque les intentions de l'agent de menace peuvent changer. Pour tenir compte de cette réalité, on doit rajuster à la baisse la probabilité d'une menace distante, tel qu'il est indiqué dans la troisième colonne du tableau C-1, afin de représenter une probabilité plus réaliste sur le site de l'EMR.

3.3.3 Biens touchés

Dans le même ordre d'idées, des menaces délibérées dirigées vers des sous-groupes de biens prévus dans un projet d'EMR sont sources de préoccupations plus sérieuses que des activités similaires visant des biens différents non prévus dans le champ d'application de l'évaluation, même s'ils se trouvent au même endroit. Néanmoins, il faut tenir compte des activités qui ont une incidence sur d'autres biens de la même catégorie puisque, encore une fois, les intentions de l'agent de menace et, par conséquent, ses cibles, peuvent changer. Par exemple, un vol de bijoux, quelle que soit sa probabilité dans un secteur donné, peut être jugé non pertinent dans le projet d'EMR d'un magasin de vêtements. Il serait prudent, toutefois, d'inclure le vol dans l'évaluation des menaces et de lui attribuer une plus faible probabilité dans la colonne 3 du tableau C-1 pour refléter les intentions actuelles.

3.3.4 Endroit et biens touchés

Finalement, une menace délibérée qui s'est matérialisée à une certaine distance et qui a eu une incidence sur des sous-groupes de biens non prévus dans le champ d'application de l'évaluation peut toujours représenter un risque crédible et justifier une entrée dans l'évaluation des menaces, même si on lui attribue une probabilité très faible sélectionnée dans la colonne 4 du tableau C-1.

3.4 Tableau des probabilités des menaces

Pour chaque incident ou activité, selon la granularité de l'analyse, déterminez la fréquence des événements passés qui, dans le champ d'application de l'évaluation, ont une incidence sur les biens dans un même endroit en utilisant les données actuarielles et les autres sources indiquées dans la liste de l'appendice C-1. Sélectionnez la gamme appropriée dans la colonne 1 pour déterminer le niveau de probabilité, de très faible à élevée, dans la colonne 2. Dans le cas où des menaces délibérées se sont manifestées ailleurs ou ont eu une incidence sur des biens non prévus dans le champ d'application de l'évaluation, choisissez le niveau approprié dans la colonne 3. Finalement, pour les menaces délibérées ayant une incidence sur des biens différents dans des endroits distants, utilisez les niveaux de probabilité de la colonne 4.

Fréquence passée	**Même endroit, biens semblables**	Endroit distant mais biens semblables ou Même endroit mais biens différents	**Endroit distant, autres biens**
Quotidienne	Élevée	Élevée	Élevée
1 à 10 jours	Élevée	Élevée	Moyenne
10 à 100 jours	Élevée	Moyenne	Faible
100 à 1 000 jours	Moyenne	Faible	Très faible
1 000 à 10 000 jours	Faible	Très faible	Très faible
Plus de 10 000 jours	Très faible	Très faible	Très faible

Tableau C-1: Tableau des probabilités des menaces

4 Évaluation de la gravité

4.1 Généralités

La conséquence ou la gravité d'un incident est une mesure de l'importance éventuelle des dommages ou de la compromission advenant que l'incident se matérialise. Dans le cas des menaces délibérées, les capacités des agents de menace au plan des connaissances, des compétences et des ressources sont de bons indicateurs du résultat prévu. Par exemple, les gangs organisés sont davantage susceptibles de causer de plus grands dommages qu'un voleur seul et inexpérimenté. Dans le cas des accidents et des risques naturels, les préjudices anticipés sont normalement directement proportionnels à l'ampleur de l'événement. Autrement dit, un tremblement de terre d'une magnitude de 8,0 sur l'échelle de Richter est plus grave qu'un tremblement d'une magnitude de 5,0 ou moins. Dans chaque cas, toutefois, l'objectif réel est d'estimer les effets probables d'un incident sur n'importe quel bien dans le champ d'application de l'évaluation.

4.2 Menaces délibérées

De manière générale, les capacités des agents de menace délibérée peuvent être évaluées au plan des compétences, des connaissances et des ressources qu'ils possèdent relativement à des incidents spécifiques ou à des scénarios de menace.

- **Compétences.** Mesure de l'aptitude de l'agent de menace à exploiter certaines vulnérabilités pour compromettre des biens dans le contexte de l'évaluation, aptitudes également appelées savoir-faire dans certains milieux. Les niveaux de compétence peuvent varier de la maîtrise absolue d'une technique donnée à la capacité modérée et à l'ineptie totale. Par exemple, les pirates de haut niveau manifestent habituellement des niveaux de compétences supérieurs alors que les jeunes néophytes tendent à se retrouver au bas du spectre; les premiers sont donc plus susceptibles de causer des dommages plus graves que les derniers s'ils décident d'attaquer une cible donnée.
- **Connaissances.** Mesure de la connaissance d'un agent de menace relativement à l'intérêt potentiel d'un bien, à sa valeur et aux vulnérabilités connexes. Bien que la connaissance soit quelque peu différente des compétences, on combine généralement les deux pour obtenir une dimension essentiellement qualitative de la capacité d'un agent de menace délibérée.
- **Ressources.** La mesure complémentaire quantitative des capacités des agents de menace inclut une évaluation des ressources financières et humaines sur lesquelles un attaquant peut compter, et de tout autre outil pertinent, telles la puissance de calcul et autres technologies évoluées, relativement aux incidents concernés.

4.3 Accidents et risques naturels

Règle générale, l'ampleur des dommages causés par un accident ou un risque naturel est directement proportionnelle à la gravité ou à l'importance de l'incident.

- **Incidence grave.** On peut s'attendre raisonnablement que l'incident soit susceptible de causer une compromission majeure, incluant la divulgation, la destruction, l'élimination, la modification ou l'utilisation non autorisées de 25 % ou plus d'un sous-groupe de biens, ou une interruption prolongée des services pendant plus de cinq jours ouvrables.
- **Incidence modérée.** On peut s'attendre raisonnablement que l'incident soit susceptible de causer une compromission sérieuse, incluant une incidence sur un maximum de 25 % d'un sous-groupe de biens, ou une interruption des services d'au moins cinq jours ouvrables.
- **Incidence restreinte.** On peut s'attendre raisonnablement que l'incident soit susceptible de causer une compromission mineure, incluant une incidence sur moins de 5 % d'un sous-groupe de biens, ou une interruption des services de moins de trois heures.

4.4 Tableau de la gravité des menaces

Dans le tableau C-2 sur la gravité des menaces, pour chaque menace qui a une incidence sur des biens dans le contexte de l'évaluation, on établit entre les capacités des agents de menace délibérée et l'ampleur des accidents et des risques naturels une correspondance à leurs incidences potentielles ou à leur gravité.

Capacités de l'agent de menace délibérée	Magnitude des accidents ou des risques naturels	**Incidence ou gravité de la menace**
Connaissances/compétences étendues et ressources considérables	Hautement destructifs Erreur extrêmement grave Utilisation abusive généralisée	Élevée
Connaissances/compétences limitées et ressources considérables **ou** Connaissances/compétences étendues et ressources limitées **ou** Connaissances/compétences modérées et ressources moyennes	Modérément destructifs Erreur grave Utilisation abusive importante	Moyenne
Connaissances/compétences limitées et ressources limitées	Peu destructifs Erreur mineure Utilisation abusive limitée	Faible

Tableau C-2 : Tableau de la gravité des menaces

5 Évaluation des menaces

5.1 Niveaux de menace

Une fois qu'on a déterminé la probabilité de la menace à l'aide du tableau C-1 et précisé sa gravité conformément au tableau C-2, on reporte ces valeurs dans le tableau C-3 pour établir la cote globale, de très faible à très élevée, de chaque menace qui a une incidence sur les biens prévus dans le champ d'application de l'évaluation.

Incidence de la menace	**Probabilité de la menace**			
	Très faible	**Faible**	**Moyenne**	**Élevée**
Élevée	Faible	Moyenne	Élevée	Très élevée
Moyenne	Très faible	Faible	Moyenne	Élevée
Faible	Très faible	Très faible	Faible	Moyenne

Tableau C-3 : Tableau des niveaux de menace

5.2 Application pratique

5.2.1 Généralités

Comme il a été expliqué précédemment, dans le cadre d'un projet d'EMR, on doit attribuer, à toutes les menaces qui ont une incidence sur des biens, une ou plusieurs cotes selon la probabilité de leur occurrence et leur incidence potentielle. Toutefois, l'évaluation des menaces peut devenir compliquée en raison d'autres considérations importantes. Par exemple, les niveaux de menace peuvent ne pas être constants. De plus, un incident donné peut avoir des conséquences multiples, soit des incidences sur plusieurs biens et valeurs de biens différents.

5.2.2 Niveaux de menace variables

Tant la probabilité que la gravité d'une menace donnée peuvent varier dans le temps. Dans le cas de plusieurs risques naturels, il existe des fluctuations saisonnières; par exemple, des inondations peuvent se produire plus fréquemment au printemps et leurs incidences peuvent alors être plus sérieuses qu'en automne ou en hiver. Dans le cas des accidents, l'heure de la journée ou le jour de la semaine peuvent être des facteurs importants puisque les gens sont plus susceptibles de commettre des erreurs lorsqu'ils sont fatigués ou exceptionnellement occupés. La probabilité de certaines menaces délibérées obéit également à certains cycles. Par exemple, l'incidence des vols à l'étalage et autres menus larcins est plus fréquente lorsque le prix des médicaments augmente dans le commerce alors que les actes de sabotage mineurs ou les dommages intentionnels sont plus fréquents durant les périodes de conflits ouvriers et lorsqu'il y a des tensions dans le milieu de travail. Dans le même ordre d'idées, les capacités des agents de menace, et par conséquent la gravité des menaces délibérées, peuvent changer lorsque ceux-ci développent de nouvelles compétences ou ont accès à davantage de ressources. De manière générale, on doit enregistrer les niveaux de menace plus élevés au cours de l'évaluation des menaces. Toutefois, lorsque des pointes se manifestent et sont facilement identifiables, on peut saisir et évaluer les deux valeurs au cours de la phase suivante du projet d'EMR afin de

déterminer les variations connexes au plan du risque global. On peut alors être en mesure de sélectionner et de recommander des mesures de protection plus ciblées et rentables au cours de la phase finale de l'évaluation.

5.2.3 Niveaux de menace multiples

En ce qui concerne les menaces délibérées, la gravité d'un incident n'est pas nécessairement la même dans différents scénarios de menace concernant des biens similaires ou différents puisque les capacités des agents de menace peuvent varier pour chaque profil d'attaque. Par exemple, un service d'espionnage peut employer entre autres des techniques de renseignement humain (HUMINT) ou de renseignement électromagnétique (SIGINT) pour compromettre la confidentialité de données sensibles, mais les compétences et les ressources employées peuvent varier de manière significative selon les différentes méthodes utilisées. Par conséquent, l'évaluation des menaces peut, inéluctablement, inclure deux niveaux de menace différents ou plus pour un même agent de menace qui cible ne serait-ce qu'un seul bien. À un niveau de granularité encore plus bas, la capacité d'un seul agent de menace d'exploiter une vulnérabilité donnée peut être très différente de sa capacité d'exploiter d'autres vulnérabilités. Donc, selon le champ d'application de l'évaluation, on peut attribuer deux niveaux de menace ou plus à un même incident, selon les divers scénarios d'exploitation de différentes vulnérabilités visant la compromission d'un seul bien. Normalement, on doit éviter ce niveau de complexité, sauf dans les situations les plus risquées où tant la valeur des biens que les menaces sont élevées.

5.2.4 Biens touchés multiples

Certains incidents sont très ciblés. Par exemple, un voleur peut s'intéresser à un seul sous-groupe de biens, telles des huiles sur toile, ou même à une seule composante, par exemple une œuvre d'art particulière. Réciproquement, d'autres incidents peuvent se répercuter sur plusieurs biens différents : un incendie criminel ou accidentel peut endommager la propriété, blesser des personnes, détruire du matériel et miner le moral ou la confiance du public. Néanmoins, un seul niveau de menace peut suffire pour évaluer les menaces et les risques, sauf lorsque la gravité de l'incident varie pour différents biens. Cela dit, on utilise toujours un seul niveau de menace lors du calcul ultérieur des risques pour chaque bien et de la combinaison des trois variables (valeur du bien, menace et vulnérabilité) au cours de la phase d'évaluation des risques du projet d'EMR.

5.2.5 Incidences multiples des menaces

La majorité des incidents compromettent la valeur, la confidentialité, la disponibilité ou l'intégrité d'un seul bien à la fois. Dans certains cas, toutefois, un incident particulier peut compromettre une deuxième valeur et, encore plus rarement, une troisième. Par exemple, un foudroiement qui crée une surcharge de tension est plus susceptible d'endommager de l'équipement délicat ou de créer une panne du système de distribution, deux problèmes liés à la disponibilité. À l'occasion, la foudre peut entraîner l'altération de données soit durant leur transmission, soit sur des supports magnétiques, deux problèmes liés à l'intégrité. On peut même concevoir qu'un même incident puisse acheminer par erreur un signal sensible à la mauvaise adresse, problème lié à la confidentialité. En fait, un incident peut avoir des incidences multiples et chacune doit être attribuée au niveau de menace approprié; elles peuvent être toutes différentes selon leur probabilité d'occurrence et la gravité de leurs conséquences.

5.2.6 Niveau de granularité

La liste hiérarchique des menaces permet la saisie et l'analyse des données à différents niveaux de granularité correspondant au champ d'application de l'évaluation. En règle générale, toutefois, il est plus probable que les données soient collectées en fonction de leurs relations aux agents de menace et à des incidents particuliers. Pour déterminer la gravité des menaces délibérées elles-mêmes, on doit évaluer les capacités des agents de menace en fonction de vulnérabilités spécifiques en utilisant des scénarios de menace encore plus détaillés; toutefois, dans la mesure du possible, les niveaux de menace doivent être intégrés à une colonne de niveau supérieur dans la liste des menaces, de préférence à la catégorie d'agent de menace, ou même à l'activité de menace, afin de réduire le nombre de variables au cours de la phase d'évaluation des risques subséquente du projet d'EMR. Évidemment, cela est possible seulement si les niveaux de menace relatifs des différents incidents d'une catégorie ou d'une activité sont relativement cohérents. Pour faciliter la tâche, lorsqu'il y a de grands écarts entre les niveaux de menace les plus élevés et les plus faibles dans une catégorie donnée, on peut toujours consolider les données le plus possible en regroupant les incidents dont les niveaux de menace sont similaires.

5.3 Résumé

La détermination des niveaux de menace selon la probabilité et la gravité des incidents, et les activités fondées sur des paramètres communs pour en permettre l'analyse comparative, sont essentiels à la méthodologie harmonisée d'EMR. Les instructions plus détaillées et les exemples à l'appendice C-3 étoffent davantage les trois dernières étapes de l'évaluation des menaces.

6 Tableau priorisé d'évaluation des menaces

Tel qu'il est indiqué ci-dessus, dans le cadre d'une évaluation, on doit attribuer un ou plusieurs niveaux de menace à toutes les menaces qui ont une incidence sur les biens selon leur probabilité d'occurrence et leur incidence potentielle. Un incident particulier est susceptible de causer un préjudice à un ou plusieurs biens et, ainsi, d'en compromettre la confidentialité, la disponibilité et (ou) l'intégrité; on doit donc déterminer les niveaux de menace pour chaque conséquence distincte. Chacun de ces niveaux doit être reporté dans le tableau d'évaluation des menaces, produit final de la phase d'évaluation des menaces d'un projet d'EMR. Le simple tri des niveaux de menace, de Très élevé à Très faible, peut permettre de prioriser rapidement les menaces et de déterminer celles qui sont les plus préoccupantes.

Cette liste est illustrée dans le tableau C-4 et étoffée à l'annexe C-4.

Classe de menace	Activité de menace	Catégorie d'agent de menace	Agent de menace	Incident	Niveaux de menace			Sous-groupe(s) de biens touchés
					C	D	I	
Légende : C – Confidentialité, D – Disponibilité, I - Intégrité								

Tableau C-4 : Exemple de tableau d'évaluation des menaces

Appendice C-1 - Sources de données sur les menaces

Ressources ministérielles	
Source de données	**Type de menace**
Gestionnaires de programme	• Perturbations dans les services • (Certaines) menaces internes • Erreurs de la part d'un employé
Gestionnaires du matériel ou des biens	• Pertes matérielles pour l'État o Vol de matériel o Perte/destruction accidentelle o Erreurs comptables
Gestionnaires des installations	• Incidents de sécurité locaux • Pannes des systèmes de chauffage, de ventilation et de climatisation • Pannes d'électricité • Inondations/autres risques environnementaux
Ressources humaines	• Violence dans le milieu de travail • Agitation ouvrière • Problèmes disciplinaires
Finances	• Toutes pertes pour l'État • Erreurs comptables
Dirigeant principal de l'information	• Défaillances au chapitre de l'intégration des systèmes
Administrateur (de la sécurité) des systèmes	• Rapports du système de détection des intrusions • Registres de vérification de la sécurité • Incidents découlant d'un code malveillant • Défaillances du matériel • Failles dans les logiciels
Agent de sécurité du ministère	• Incidents/enquêtes concernant la sécurité • Rapports de renseignement de sécurité de l'organisme responsable
Coordonnateur de la sécurité des TI	• Incidents/enquêtes concernant la sécurité des TI
Coordonnateur, PCA	• Urgences/incidents majeurs
Vérification interne/examen	• Mauvaise gestion interne • Rapports de vérification judiciaire
Conseiller juridique	• Poursuites contre l'État
Santé et sécurité au travail	• Accidents • Risques pour la santé

Ressources externes : Ministères responsables en matière de sécurité	
Source de données	**Type de menace**
Service canadien du renseignement de sécurité http://www.csis-scrs.gc.ca/fr/index.asp	• Documents des séries *Commentaire* ou *Perspectives*, non classifiées • Évaluations de la menace, classifiées o Espionnage o Sabotage o Activités clandestines pour le compte d'une entité étrangère o Terrorisme
Centre de la sécurité des télécommunications http://www.cse-cst.gc.ca/index-f.html	• Incidents COMSEC • Alertes/Bulletins concernant la sécurité des TI • Renseignement étranger (SIGINT)
Affaires étrangères et Commerce international Canada http://www.voyage.gc.ca/main/before/faq/tip-fr.asp	o Programme de renseignements aux voyageurs o Dernières nouvelles o Avertissements o Menaces à l'étranger
Sécurité publique et Protection civile Canada http://www.ps-sp.gc.ca/index-fr.asp	• Centre canadien de réponse aux incidents cybernétiques • Les *Résumés quotidiens* de SPPCC o Accidents ou risques naturels o Incidents de sécurité des TI
Travaux publics et Services gouvernementaux Canada Gardiens d'immeuble	• Incidents de sécurité locaux • Pannes des systèmes de chauffage, de ventilation et de climatisation • Pannes d'électricité • Inondations/autres risques environnementaux
Gendarmerie royale du Canada http://www.rcmp-grc.gc.ca/crimint/reports_f.htm	• Rapports de la Direction des renseignements criminels

Ressources externes : autres organismes gouvernementaux	
Source de données	**Type de menace**
Centre canadien d'hygiène et de sécurité au travail du Canada http://www.ccohs-cchst.gc.ca/	• Risques biologiques • Maladies et lésions • Rapports sur la santé et la sécurité
Environnement Canada http://www.ec.gc.ca/default.asp?lang=fr	• Archives nationales d'information et de données climatologiques • Inventaire national des rejets de polluants

Santé Canada http://www.hc-sc.gc.ca/index_f.html	• Risques pour la santé et la sécurité • Avis, mises en garde et retraits
Service météorologique du Canada http://www.msc-smc.ec.gc.ca/contents_f.html?	• Conditions météorologiques (extrêmes)

Ressources externes : Autres organismes du secteur public	
Source de données	**Type de menace**
Conseil canadien des directeurs provinciaux et des commissaires des incendies http://www.ccfmfc.ca/	• Sinistres attribuables à des incendies au Canada
Service d'incendie local	• Incendies accidentels/criminels
Service de police local	• Menaces d'origine criminelle
Gouvernements provinciaux	• Interruptions de travail
Services publics	• Interruptions de l'électricité ou de l'eau

Ressources externes : Secteur privé	
Source de données	**Type de menace**
Secteur de l'assurance	• Menaces diverses
Fournisseurs de services	• Perturbations dans les services
Fournisseurs de produits	• Défaillances du matériel • Failles dans les logiciels

Ressources externes : Journaux professionnels
American Intelligence Journal http://www.nmia.org/
Canadian Geographic http://www.canadiangeographic.ca
Competitive Intelligence Magazine http://www.scip.org
Journal of Competitive Intelligence and Management http://www.scip.org
Computer Fraud and Security http://www.elsevier.com/wps/find/journaldescription.cws_home/405876/description#description
Contingency Planning and Management (CPM) Magazine http://www.contingencyplanning.com
Counterintelligence News and Developments Newsletter http://www.loyola.edu/dept/politics/hula/cind1.html

Cryptologia Journal http://www.dean.usma.edu/math/pubs/cryptologia
Defense Intelligence Journal http://www.ndicfoundation.org/xp/ndic/content/dij/
Disaster Recovery Journal http://www.drj.com/drj2/drj2.htm
Global Crime http://www.tandf.co.uk/journals/titles/17440572.asp
Intelligence and National Security http://www.routledgestrategicstudies.com/journals.asp
International Journal of Intelligence & Counterintelligence http://www.tandf.co.uk/journals/tf/08850607.html
Jane's Information Group http://www.janes.com
Journal of Safety Research http://www.elsevier.com/wps/find/journaldescription.cws_home/679/description#description
Journal of Strategic Studies http://www.tandf.co.uk/journals/titles/01402390.asp
Security Studies http://www.tandf.co.uk/journals/titles/09636412.asp
Small Wars & Insugencies http://www.tandf.co.uk/journals/titles/09592318.asp
Studies in Conflict and Terrorism http://www.tandf.co.uk/journals/titles/1057610X.asp
Studies in Intelligence https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/index.html
Terrorism and Political Violence http://www.tandf.co.uk/journals/titles/09546553.asp

Nota :

1. Cette liste n'est pas exhaustive. D'autres éléments s'y ajouteront occasionnellement. Toute suggestion de documents de référence ou de contacts à ajouter peut être présentée aux bureaux mentionnés dans l'Avant-propos.
2. L'inclusion d'une revue professionnelle ou d'un site Web ne doit pas être interprétée comme une approbation. De la même manière, l'exclusion d'autres sources qui pourraient se révéler utiles ne signifie pas qu'elles sont rejetées. La liste vise simplement à illustrer la richesse des renseignements facilement accessibles aux spécialistes de la sécurité et aux gestionnaires de risques.

Appendice C-2 – Liste des menaces

	Classe	Activité	Catégorie d'agent	Agent	Incident
1.	Menaces délibérées	Guerre	États-nations	Nations	Invasion militaire
2.					Opérations d'information
3.			Révolutionnaires	Factions	Insurrection
4.			Rebelles	Factions	Guérilla
5.		Espionnage	Services de renseignement hostiles	Services	COMINT
6.					ELINT
7.					FISINT
8.					Interception des émissions
9.					Exploitation des réseaux
10.					HUMINT
11.					IMINT
12.					Collecte à partir de sources ouvertes
13.					Entrée par effraction
14.			Autres agents parrainés par un État	Organismes	Reprendre 8-13.
15.			Médias	Entreprises	HUMINT
16.					Veille concurrentielle
17.				Particuliers	HUMINT
18.					Veille concurrentielle
19.			Espions industriels	Entreprises	HUMINT
20.					Écoute téléphonique
21.					Écoute électronique
22.					Partenariats d'affaires
23.					Rétroingénierie
24.					Veille concurrentielle
25.					Entrée par effraction
26.				Particuliers	HUMINT
27.					Veille concurrentielle
28.					Entrée par effraction
29.			Pirates informatiques	Groupes	Exploitation des réseaux
30.					Ingénierie sociale
31.				Particuliers	Exploitation des réseaux
32.					Ingénierie sociale
33.			Crime organisé	Groupes	HUMINT
34.					Écoute électronique
35.					Exploitation des réseaux
36.		Sabotage	Parrainé par l'État	Organismes	Opérations d'information
37.			Concurrents	Organismes	Trafiquage de produit
38.			Employés mécontents	Groupes/Particuliers	Griefs frivoles
39.					Vandalisme
40.					Suppression/destruction de fichiers

	Classe	Activité	Catégorie d'agent	Agent	Incident
41.					Données altérées
42.					Chiffrement de fichiers
43.					Logiciel mal configuré
44.					Matériel mal configuré
45.			Activistes de l'extérieur	Énumérer les groupes	Destruction d'équipement
46.			Pirates informatiques	Pirates en herbe	Attaques par déni de service
47.					Code malveillant
48.					Altération de fichiers
49.				Pirates amateurs	Reprendre 46-48.
50.				Pirates compétents	Reprendre 46-48.
51.				Pirates d'élite	Reprendre 46-48.
52.		Subversion	Parrainés par l'État	Organismes	Propagande
53.			Activistes politiques	Groupes	Distribution de pamphlets
54.					Intimidation d'employés
55.			Lobbyistes	Groupes	Moyens de pression
56.				Particuliers	Subornation
57.			Concurrents	Organismes	Propagation de rumeurs
58.					Publicité (mensongère)
59.			Agitation ouvrière	Groupes	Manifestations
60.			Pirates informatiques	Pirates amateurs	Dégradation de sites Web
61.					Canulars
62.				Pirates compétents	Reprendre 60-61.
63.				Pirates d'élite	Reprendre 60-61.
64.		Terrorisme	Terroristes internationaux	Groupes	Assassinat
65.					Kidnapping
66.					Bombardement
67.					Détournement d'avion
68.					Agents chimiques
69.					Agents nucléaires
70.					Collecte de fonds
71.					Recrutement
72.					Formation
73.					Blanchiment d'argent
74.			Terroristes nationaux	Énumérer les groupes	Lettre piégée
75.					Bombe incendiaire
76.					Bombe tuyau
77.		Actes criminels	Menaces internes	Employés	Incendie criminel
78.					Agression
79.					Violation de droits d'auteur
80.					Extorsion
81.					Falsification de documents
82.					Fraude
83.					Homicide
84.					Dommages matériels
85.					Subornation
86.				Employés temporaires	Reprendre 77-85.
87.				Sous-traitants	Reprendre 77-85.
88.				Personnel d'entretien	Reprendre 77-85.
89.				Gardiens de sécurité	Reprendre 77-85.

	Classe	Activité	Catégorie d'agent	Agent	Incident
90.			Menaces externes	Clients	Reprendre 77-85.
91.				Entrepreneurs	Reprendre 77-85.
92.				Visiteurs	Reprendre 77-85.
93.				Public	Reprendre 77-85.
94.				Pirates informatiques	Vol d'identité
95.				Jeunes contrevenants	Graffitis
96.					Vandalisme
97.				Petits truands	Vol
98.					Cambriolage
99.			Crime organisé	Groupes	Jeux de hasard
100.					Blanchiment d'argent
101.					Trafic de stupéfiants
102.					Vol d'identité
103.			Concurrents	Entreprises	Contrefaçon de brevet
104.					Violation de droits d'auteur
105.					Influence des marchés publics
106.		Autres	Polluposteurs	Particuliers	Pourriels
107.			Employés	Particuliers	Navigation constante sur le Web
108.					Utilisation non autorisée
109.					Absentéisme
110.			Mouvements ouvriers/ Syndicats	Groupes	Grève du zèle
111.					Ralentissements de travail
112.					Arrêts de travail
113.					Accès bloqué/retardé
114.			Manifestants	Groupes activistes	Marches pacifiques
115.					Routes bloquées
116.					Confrontations violentes
117.					Émeutes
118.					Occupation d'immeubles
119.				Groupes ethniques	Reprendre 114-118.
120.				Mouvements ouvriers	Reprendre 114-118.
121.	Menaces accidentelles	Accidents au bureau	Employés	Personnel de bureau	Fichiers supprimés
122.					Dégâts de café/d'autres liquides
123.					Trébuchement/Blessure
124.					Courrier mal acheminé
125.					Mot de passe oublié
126.				Personnel de nettoyage	Équipement débranché
127.		Biens perdus	Employés	Particuliers	Ordinateur portatif perdu
128.			Entrepreneurs	Organismes	Livraisons mal acheminées
129.		Altération des données	Employés	Commis à la saisie des données	Erreurs de saisie de donnée
130.				Administrateurs de bases de données	Erreurs d'exploitation
118.			Clients	Particuliers	Saisie de données inexactes
131.		Failles dans un logiciel	Fournisseurs de logiciels	Entreprises	Bogues informatiques

	Classe	Activité	Catégorie d'agent	Agent	Incident
132.			Intégrateurs de systèmes	Organismes	Erreurs d'intégration de systèmes
133.			Programmeurs internes	Particuliers	Erreurs de codage
134.			Administrateurs de systèmes	Particuliers	Erreurs de configuration de logiciels
135.		Défaillances du matériel	Fournisseurs de matériel	Entreprises	Vices de conception
136.					Défectuosité de l'équipement
137.			Intégrateurs de systèmes	Organismes	Erreurs d'installation
138.			Administrateurs de systèmes	Particuliers	Erreurs de configuration du matériel
139.					Erreurs/mauvaise utilisation de la part des opérateurs
140.		Défaillances mécaniques	Fournisseurs d'équipement	Entreprises	Vices de conception
141.					Défaillances de l'équipement
142.			Services publics	Compagnies	Interruption de l'eau
143.					Panne d'électricité
144.			Gardiens d'immeuble	Préposés à l'entretien des SCVC	Perte de chauffage
145.					Condensation
146.				Plombiers	Fuites/dégâts d'eau
147.			Opérateurs d'équipement	Particuliers	Mauvaise utilisation par inadvertance
148.		Défaillances de structure	Architectes	Entreprises	Vices de conception
149.			Industrie du bâtiment	Entreprises	Construction non conforme aux normes
150.			Occupants d'immeuble	Organismes	Surcharge des planchers
151.		Incendies	Employés	Fumeurs	Cigarettes mal éteintes
152.				Personnel de nettoyage	Combustion spontanée
153.				Électriciens	Court-circuit
154.		Accidents industriels	Travailleurs du secteur des transports	Camionneurs	Déversement toxique
155.			Équipes de fabrication	Opérateurs d'équipement	Blessures
156.					Production perturbée
157.		Accidents routiers	Employés	Particuliers	Accident de la route – véhicule privé
158.				Routiers	Accident de la route – véhicule de transport public
159.		Accidents nucléaires	Centrale nucléaire	Personnel de l'exploitation	Fuite de radiations
160.					Fusion du cœur d'un réacteur
161.			Installations médicales	Personnel médical	Surdose accidentelle
162.	Risques naturels	Maladies	Bactéries	Staphylocoques	Empoisonnement alimentaire
163.				Autres bactéries	Pandémie
164.					Épidémie
165.					Éclosion locale
166.					Infection individuelle

	Classe	Activité	Catégorie d'agent	Agent	Incident
167.			Spirochètes	Syphilis	Infection individuelle
168.				Autres spirochètes	Reprendre 163-166.
169.			Virus	Grippe aviaire	Reprendre 163-166.
170.				Autres virus	Reprendre 163-166.
171.			Infections fongiques	Histoplasmose	Maladie grave/Décès
172.				Autres champignons	Maladie/Décès
173.			Parasites	Malaria	Maladie/Décès
174.				Autres parasites	Maladie/Décès
175.			Cancers	Leucémie	Maladie prolongée/Décès
176.				Autres cancers	Maladie/Décès
177.			Maladies cardiaques	Crise cardiaque	Invalidité/Décès
178.				ACV	Invalidité/Décès
179.		Mouvements de terrain	Érosion	Érosion due à l'eau	Immeuble sapés
180.				Érosion due au vent	Décapage de la terre végétale
181.			Tassements de terrain	Perte d'eaux souterraines	Immeuble sapés
182.					Routes effondrées
183.					Inondation locale
184.				Roche carbonatée	Reprendre 181-183.
185.			Glissements de terrain	Infiltration d'eaux pluviales	Écroulement des bâtisses
186.					Perturbation du transport
187.				Érosion due à l'eau	Reprendre 185-186.
188.			Volcans	Coulées de lave	Immeubles détruits
189.					Déplacements perturbés
190.					Blocage de l'écoulement de l'eau
191.				Cendres volcaniques	Immeubles enterrés
192.					Suffocation des gens
193.					Contamination de l'eau
194.			Séismes	Séismes interplaque	Micro (2,0 à l'Échelle de Richter)
195.					Mineur (2,0 – 3,9)
196.					Léger (4,0 – 4,9)
197.					Modéré (5,0 – 5,9)
198.					Fort (6,0 – 6,9)
199.					Majeur (7,0 – 7,9)
200.					Important (8,0 – 8,9)
201.					Exceptionnel (9,0 – 9,9)
202.				Séismes intraplaque	Reprendre 194-201
203.		Inondations	Lacs	Propre au site	Ruissellement du printemps
204.					Embâcle
205.					Crue soudaine
206.			Rivières/fleuves	Propre au site	Reprendre 203-205.
207.			Océans	Propre au site	Grande marée
208.		Activité d'ordre environnemental	Particules en suspension dans l'air	Poussière	Contamination des matières filtrantes
209.				Pollen	Réactions allergiques
210.			Température	Vague de chaleur	Déshydratation/Décès

	Classe	Activité	Catégorie d'agent	Agent	Incident
211.				Froid extrême	Engelures
212.				Froid prolongé	Pertes de vie
213.			Humidité	Forte humidité	Pourriture sèche /Dommages structurels
214.					Spores/Réactions allergiques
215.				Faible humidité	Électricité statique
216.			Magnétisme	Géomagnétisme	Entraves à la navigation
217.			Radiations	Radon	Danger pour la santé
218.			Électricité statique	Décharges d'électricité statique	Altération des fichiers
219.			Phénomènes stellaires	Rayons cosmiques	Dégradation des piles solaires
220.				Météores	Dégradation des satellites
221.				Lumière du soleil	Grave coup de soleil
222.					Dégradation des tissus exposés
223.				Tempêtes géomagnétiques	Communications perturbées
224.					Pannes d'électricité
225.		Violentes tempêtes	Vents violents	Ouragans	Catégorie 1 à l'Échelle de Saffir-Simpson
226.					Catégorie 2 à l'Échelle de Saffir-Simpson
227.					Catégorie 3 à l'Échelle de Saffir-Simpson
228.					Catégorie 4 à l'Échelle de Saffir-Simpson
229.					Catégorie 5 à l'Échelle de Saffir-Simpson
230.				Tornades	F0 à l'Échelle de Fujita
231.					F1 à l'Échelle de Fujita
232.					F2 à l'Échelle de Fujita
233.					F3 à l'Échelle de Fujita
234.					F4 à l'Échelle de Fujita
235.					F5 à l'Échelle de Fujita
236.					F6 à l'Échelle de Fujita
237.				Typhons	Reprendre 225-229.
238.			Orages	Foudre	Hausses de tension électrique
239.					Pannes d'électricité
240.					Incendies
241.				Pluies intenses	Inondations
242.			Tempêtes de neige	Chutes de neige abondantes	Congestion de la circulation/ Retards
243.					Pannes d'électricité
244.			Tempêtes de grêle	Gros grêlons	Dommages aux récoltes
245.			Pluie verglaçante	Accumulation de glace	Chutes/Blessures
246.					Accidents routiers
247.					Pannes d'électricité
248.		Animaux	Gros mammifères	Chevreuils	Collision avec un véhicule
249.			Rongeurs	Écureuils	Isolant rongé
250.			Oiseaux	Mouettes	Impacts d'oiseaux
251.			Reptiles	Serpents	Morsures

	Classe	Activité	Catégorie d'agent	Agent	Incident
252.			Poissons	Requins	Attaques par un requin
253.			Insectes	Tiques	Vecteur de la maladie de Lyme
254.		Plantes	Mauvaises herbes	Divers	Plantes indigènes remplacées par les mauvaises herbes
255.			Plantes toxiques	Herbe à puce	Contact individuel
256.				Rhus diversiloba	Contact individuel
257.				Sumac à vernis	Contact individuel
258.			Plantes vénéneuses	Algues	Contamination de l'eau
259.				Champignons	Empoisonnements
260.				Plantes feuillues	Empoisonnements

Nota :

1. De toute évidence, la liste des menaces n'est pas exhaustive et ne pourra jamais l'être. De nouvelles menaces apparaissent régulièrement, en particulier au niveau de l'incident. Par conséquent, d'autres éléments seront ajoutés occasionnellement à la liste. Toute suggestion d'ajout peut être présentée aux bureaux mentionnés dans l'Avant-propos.
2. Lorsqu'une évaluation des menaces est réalisée dans le cadre d'un projet d'EMR, toutes les menaces visées par l'évaluation peuvent être transférées, au niveau de ventilation qui convient, de la liste ci-dessus aux cinq premières colonnes du tableau d'évaluation des menaces de l'appendice C-4.

Page intentionnellement laissée en blanc

Appendice C-3 - Paramètres des menaces

1 Instructions

Dans le cadre du projet d'EMR, il faut déterminer le niveau approprié de chaque menace évaluée en procédant ainsi :

- **Étape 1.** Déterminez le niveau de ventilation, ou granularité, pertinent (activité, catégorie d'agent, agent ou incident) de chaque entrée en fonction des critères de définition de la portée figurant à la section 4 de l'annexe A.
- **Étape 2.** Pour chaque menace, évaluez la probabilité d'occurrence sur une échelle allant de très faible à très élevée, d'après les renseignements courants ou des lectures de capteurs, le cas échéant, ou encore, dans la plupart des cas, à partir de l'expérience antérieure et de données actuarielles –
    - sélectionnez la fréquence qui correspond le plus étroitement aux événements antérieurs dans la colonne 1 du tableau C3-1, Tableau des probabilités des menaces;
    - pour toutes les menaces (menaces délibérées, menaces accidentelles et risques naturels) qui s'appliquent aux sous-groupes des biens visés par l'évaluation dans un même emplacement, déterminez la probabilité correspondante selon la colonne 2 puis passez à la troisième étape;
    - dans le cas des menaces délibérées toutefois, les intentions des agents peuvent changer au fil du temps, de sorte que les menaces qui s'appliquent à certains sous-groupes de biens et certains emplacements qui ne sont pas visés par l'évaluation pourront soulever des préoccupations à l'avenir, et il conviendrait de rajuster en conséquence les probabilités qui s'y rapportent –
        - pour les menaces qui s'appliquent à des sous-groupes de biens n'étant pas visés par l'évaluation mais qui se trouvent à un même endroit, sélectionnez le niveau de la colonne 3 qui correspond à la fréquence antérieure indiquée dans la colonne 1;
        - de la même façon, pour les menaces qui s'appliquent à des sous-groupes de biens visés par l'évaluation qui se trouvent dans différents endroits ne rentrant pas dans le cadre du projet d'EMR, sélectionnez le niveau de la colonne 3 qui correspond à la fréquence antérieure indiquée dans la colonne 1;
        - pour les menaces qui s'appliquent à des sous-groupes de biens non visés par l'évaluation et qui se trouvent dans des endroits différents, sélectionnez le niveau de la colonne 4 qui correspond à la fréquence antérieure indiquée dans la colonne 1.

Colonne 1	Colonne 2	Colonne 3	Colonne 4
Fréquence antérieure	Même endroit, biens semblables	Endroit distant mais biens semblables ou Même endroit mais biens différents	Endroit distant, autres biens
Quotidienne	Élevée	Élevée	Élevée
1 à 10 jours	Élevée	Élevée	Moyenne
10 à 100 jours	Élevée	Moyenne	Faible
100 à 1 000 jours	Moyenne	Faible	Très faible
1 000 à 10 000 jours	Faible	Très faible	Très faible
Plus de 10 000 jours	Très faible	Très faible	Très faible

Tableau C3-1 : Tableau des probabilités des menaces

- **Étape 3.** Déterminez la gravité possible des menaces susceptibles de se concrétiser d'après les capacités des agents ou la magnitude des accidents et des risques naturels, et attribuez-lui le niveau approprié sur une échelle allant de faible à élevée dans le tableau C3-2, Tableau de la gravité des menaces.

Capacité de l'agent de menace délibérée	Magnitude des accidents ou des risques naturels	Incidence ou gravité de la menace
Connaissances/compétences étendues et ressources importantes	Hautement destructifs Erreur extrêmement grave Utilisation abusive généralisée > 25 % du sous-groupe de biens touchés Interruptions > 5 jours ouvrables	Élevée
Connaissances/compétences limitées et ressources considérables ou Connaissances/compétences étendues et ressources limitées ou Connaissances/compétences modérées et ressources moyennes	Modérément destructifs Erreur grave Utilisation abusive importante > 5 % du sous-groupe de biens touchés Interruptions > 3 jours ouvrables	Moyenne
Connaissances/compétences limitées et ressources limitées	Peu destructifs Erreur mineure Utilisation abusive limitée < 5 % du sous-groupe de biens touchés Interruptions < 3 jours ouvrables	Faible

Tableau C3-2 : Tableau de la gravité des menaces

- **Étape 4.** Déterminez le niveau de chaque menace sur une échelle allant de Très faible à Très élevé en mettant en corrélation la probabilité de la menace (axe horizontal du tableau C3-3, Tableau des niveaux de menace) et l'incidence (ou gravité) de la menace (axe vertical).

Incidence de la menace	Probabilité de la menace			
	Très faible	**Faible**	**Moyenne**	**Élevée**
Élevée	Faible	Moyenne	Élevée	Très élevée
Moyenne	Très faible	Faible	Moyenne	Élevée
Faible	Très faible	Très faible	Faible	Moyenne

Tableau C3-3 : Tableau des niveaux de menace

- **Étape 5a.** Selon la nature de la compromission prévue, entrez les résultats dans les colonnes des niveaux appropriés de la confidentialité, de la disponibilité et/ou de l'intégrité du tableau d'évaluation des menaces de l'appendice C-4.
- **Étape 5b.** S'il vous reste un doute au sujet du niveau réel de la menace, vous pouvez entrer la valeur la plus élevée et la valeur la plus faible dans le tableau d'évaluation des menaces et les utiliser pour calculer le risque résiduel dans la phase d'évaluation des risques (annexe E), afin de déterminer si cette incertitude se répercute sur le niveau de risque résiduel.
- **Étape 5c.** Si une menace se rapproche de la ligne de démarcation entre deux niveaux, il convient de la baliser au moyen de flèches (↑↓) indiquant si elle se rapproche de l'extrémité supérieure ou de l'extrémité inférieure de la fourchette; elle pourra ainsi faire l'objet d'une analyse subséquente lors de la phase d'évaluation des risques du projet d'EMR. Par exemple, si la fréquence antérieure d'une menace était d'une fois tous les 110 jours, en d'autres termes si sa probabilité est moyenne mais se rapproche de la probabilité élevée, le niveau final de la menace devrait être marqué d'une flèche ascendante (↑).
- **Étape 5d.** Lorsque la probabilité d'une menace délibérée est faible ou moyenne, il convient de calculer un second niveau de menace en lui attribuant une probabilité élevée, puis d'utiliser ce second niveau pour calculer un second risque résiduel pendant la phase d'évaluation des risques; en effet, les intentions des agents peuvent changer beaucoup plus rapidement que ne peuvent se faire l'acquisition et l'installation des contre-mesures nécessaires.
- **Étape 6.** Entrez les résultats dans les colonnes appropriées du tableau d'évaluation des menaces de l'appendice C-4.

2 Exemples

2.1 Vol

S'il a eu vol de fournitures de bureau et d'objets personnels chaque semaine depuis un an dans des locaux du gouvernement dans le secteur immédiat visé par un projet d'EMR, la probabilité que se produisent d'autres incidents concernant d'autres biens du même genre serait élevée. Si

les coupables étaient généralement des personnes dont les connaissance, les compétences et les ressources ne sont que moyennes, la gravité serait moyenne, et le niveau global de la menace serait élevé pour ce qui est de la disponibilité des biens en question.

2.2 Vol à main armée

Si les entreprises locales du secteur privé ont été victimes de vols à main armée toutes les deux ou trois semaines, la probabilité que se produisent d'autres incidents du même genre à l'avenir serait élevée. Toutefois, si les bureaux du gouvernement n'ont pas été visés, la probabilité relative doit être tempérée; la colonne 3 du tableau C3-1 (Même endroit mais biens différents) permet d'arriver à une probabilité moyenne. Si ces vols à main armée ont été commis par des gangs bien organisés qui possèdent des connaissances, des compétences et des ressources significatives, la gravité serait élevée, et le niveau global de la menace serait élevé pour ce qui est de la disponibilité des biens dans les installations du gouvernement et très élevée dans le secteur privé.

2.3 Erreurs d'acheminement de courriels

Si des employés négligents expédient un message Protégé A aux mauvais destinataires environ une ou deux fois par année, la probabilité que ce genre d'incident se reproduise serait moyenne. Si de telles erreurs concernent moins de 1 % de tous les messages Protégé A, la gravité serait faible, ce qui donnerait une menace accidentelle de faible niveau en matière de confidentialité.

2.4 Inondations

Si des inondations localisées perturbent généralement les opérations pendant trois ou quatre jours au cours d'une année, la probabilité d'interruptions futures serait moyenne, car une fréquence de quatre fois pendant l'année représente moins d'une fois tous les 100 jours sur toute l'année. Si l'impact se traduit par une perte de productivité de moins de 10 %, la gravité de la menace serait moyenne, et le niveau global de la menace serait moyen pour la disponibilité des services touchés.

Appendice C-4 - Tableau d'évaluation des menaces

Classe de menace	Activité de menace	Catégorie d'agent de menace	Agent de menace	Incident	Niveaux de menace			Sous-groupe(s) de biens touchés
					C	D	I	
Délibérées	Espionnage							
	Sabotage							
	Subversion							
	Terrorisme							
	Actes criminels							
	Autres							
Accidentelles	Accidents au bureau							
	Altération des données							
	Failles dans un logiciel							
	Défaillances du matériel							
	Défaillances mécaniques							
	Défaillances de structure							
	Incendies							
	Accidents industriels							
	Accidents nucléaires							
Risques naturels	Maladies							
	Mouvements de terrain							
	Inondations							
	Activités d'ordre environnemental							
	Violentes tempêtes							
	Plantes et animaux							

Légende :
C – Confidentialité, D – Disponibilité, I - Intégrité

1 Instructions

Entrez toutes les menaces visées par le projet d'EMR au niveau de ventilation appropriée (Activité de menace, Catégorie d'agent de menace, Agent de menace et Incident) à partir de la liste des menaces de l'appendice C-2.

À partir des paramètres des menaces de l'appendice C-3, déterminez les niveaux pertinents de chaque menace sur une échelle allant de Très faible à Très élevé (TF à TE) pour les aspects confidentialité (C), disponibilité (D) et /ou intégrité (I) des sous-groupes de biens touchés.

2 Exemples

2.1 Espionnage

Si la menace d'espionnage que pose tel ou tel service de renseignement est élevée pour la confidentialité de plans militaires en fonction de la probabilité d'occurrence et des capacités de l'adversaire, le tableau d'évaluation des menaces se présenterait ainsi :

Classe de menace	Activité de menace	Catégorie d'agent de menace	Agent de menace	Incident	Niveaux de menace			Sous-groupe(s) de biens touchés
					C	D	I	
Menaces délibérées	Espionnage	Services de renseignement	Spécifique	–	E			Plans militaires

2.2 Pirate

Si la menace que représente un pirate informatique pour les fichiers de données d'un ministère est moyenne au chapitre de l'accès non autorisé (Confidentialité) et de la modification non autorisée (Intégrité), mais élevée en ce qui concerne les attaques de déni de service (Disponibilité), le tableau d'évaluation des menaces se présenterait ainsi :

Classe de menace	Activité de menace	Catégorie d'agent de menace	Agent de menace	Incident	Niveaux de menace			Sous-groupe(s) de biens touchés
					C	D	I	
Menaces délibérées	Espionnage	Pirates informatiques	–	Accès non autorisé	M	–	–	Fichiers de données du ministère
	Sabotage	Pirates informatiques	–	Modification non autorisée	–	–	M	Fichiers de données du ministère
	Sabotage	Pirates informatiques	–	Déni de service	–	E	–	Fichiers de données du ministère

2.3 Hausses de tension

Si la menace de hausses de tension périodiques qui occasionneraient des dommages à des appareils électriques délicats est élevée (Disponibilité) mais que le risque d'altération des données qui l'accompagne est faible (Intégrité), le tableau d'évaluation des menaces se présenterait ainsi :

Classe de menace	Activité de menace	Catégorie d'agent de menace	Agent de menace	Incident	Niveaux de menace			Sous-groupe(s) de biens touchés
					C	D	I	
Menaces accidentelles	Défaillances mécaniques	Services publics	Compagnie d'électricité	Hausse de tension	–	E	–	Appareils électriques
Menaces accidentelles	Défaillances mécaniques	Services publics	Compagnie d'électricité	Hausse de tension	–	–	F	Fichiers de données

Page intentionnellement laissée en blanc

Annexe D – Évaluation des vulnérabilités

1 Introduction

1.1 Généralités

La quatrième phase d'un projet d'EMR, l'évaluation des risques, est menée en deux volets séquentiels, soit l'évaluation des vulnérabilités et le calcul des risques résiduels. Le premier volet compte cinq processus successifs et un résultat important, soit :

- **Recensement des mesures de protection –** établir une liste de toutes les mesures de protection existantes et proposées comprises dans la portée de l'évaluation, selon un degré de détail approprié.
- **Évaluation de l'efficacité des mesures de protection –** déterminer l'efficacité des mesures de protection pour réduire les risques éventuels.
- **Identification des vulnérabilités –** recenser d'autres vulnérabilités qui exposent les biens compris dans la portée de l'évaluation aux menaces cernées dans le cadre de la troisième phase.
- **Analyse de l'incidence des vulnérabilités** – évaluer les effets des vulnérabilités sur la probabilité de réalisation des menaces, la probabilité de compromission et la gravité des dommages qui en découlent.
- **Évaluation des vulnérabilités** – attribuer des cotes relatives (de « très faible » à « très élevée ») à chacune des vulnérabilités, en fonction de paramètres communs pour l'exposition accrue à un risque de compromission de la confidentialité, de la disponibilité ou de l'intégrité.
- **Tableau priorisé d'évaluation des vulnérabilités** – produire une liste exhaustive des vulnérabilités, classées en ordre décroissant de gravité.

1.2 But

Le but de cette annexe est de décrire les cinq processus et le résultat unique de l'évaluation des vulnérabilités de la phase d'évaluation des risques d'un projet d'EMR.

2 Recensement des mesures de protection

2.1 Définition de « mesure de protection »

Les mesures de protection sont des mécanismes ou des contrôles de sécurité qui remplissent une ou plusieurs fonctions dans l'atténuation du risque global en réduisant les valeurs des biens, les menaces ou les

***Mesures de protection** (safeguards)* – Biens ou contrôles externes qui réduisent les risques globaux à l'égard des employés, d'autres biens ou de la prestation des services en abaissant la probabilité des incidents ou des compromissions ou en atténuant la gravité des conséquences par l'interaction directe ou indirecte avec les valeurs d'un bien, les menaces ou les vulnérabilités.

Nouvelle définition

vulnérabilités comprises dans la portée d'un projet d'EMR. Cette réduction des variables principales du risque vise en premier lieu à diminuer la probabilité qu'une menace se concrétise, à réduire la probabilité de compromission au cas où un incident se produirait, et à restreindre la gravité des conséquences, comme le précise la nouvelle définition ci-contre.

2.2 Liste des mesures de protection

Pour évaluer les vulnérabilités exposant à un risque accru les biens inclus dans la portée d'un projet d'EMR, il faut d'abord recenser les mesures de protection existantes et proposées, puis les analyser pour en déterminer l'efficacité relative. Comme la plupart des mesures ou des mécanismes de sécurité constituent aussi des biens, bon nombre devraient avoir été déterminés à l'occasion de la phase d'identification des biens. En complément, il convient toutefois de consulter les étapes de la phase des recommandations d'un projet d'EMR, à l'annexe F, où on trouve une orientation détaillée, notamment sur l'examen des mesures de protection et des critères de sélection de ces mesures afin de tenir compte de tous les risques résiduels jugés inacceptables. Quelques sources utiles de données sur les mesures de protection sont citées à l'appendice F-1, et on présente à l'appendice F-2 une liste détaillée des mesures de sécurité servant d'aide-mémoire pour faciliter le recensement des mesures de protection dans le cadre de l'évaluation des vulnérabilités.

3 Efficacité des mesures de protection

3.1 Généralités

En règle générale, les vulnérabilités et les risques qui en découlent sont inversement proportionnels à l'efficacité des mesures de protection. En gros, plus les mesures de sécurité mises en œuvre pour protéger les biens visés par une évaluation sont robustes, plus les vulnérabilités et les risques connexes ont tendance à diminuer. En vertu de la méthodologie harmonisée d'EMR, deux facteurs sont pris en compte dans l'évaluation de l'efficacité des mesures de protection. Tout d'abord, les fonctions de sécurité que jouent toutes les mesures de protection indiquent comment celles-ci interagissent avec les principales variables de risque, à savoir les valeurs des biens, les menaces et les vulnérabilités. Ensuite, leurs répercussions sur les incidents, notamment la probabilité d'occurrence, la probabilité de compromission et la gravité des conséquences, sont examinés afin de déterminer l'efficacité globale des mesures.

3.2 Fonctions de sécurité : Incidence sur les variables de risque

En reconnaissance du fait que la gestion des risques nécessite l'acceptation de certains risques, et de la possibilité que certaines menaces causent des préjudices aux employés ou aux biens et perturbent la prestation des services, la PGS introduit la notion de défense active, notamment en ce qui a trait aux biens de TI, afin de « prévenir et détecter les incidents, y réagir et revenir aux opérations normales »[1] . De fait, la plupart des mesures de protection ont une ou plusieurs

[1] La **section 10.12 de la PGS** définit cette exigence, qui est étoffée à la **section 15 de la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)***.

fonctions de sécurité de base, soit la prévention, la détection, la réaction et la reprise. Deux autres options, l'évitement et la dissuasion, doivent également être prises en compte pour obtenir un modèle complet.

- **Évitement.** Dans certains cas, il est possible de réduire ou d'éliminer un risque en réduisant les valeurs d'un bien. Par exemple, la plupart des dépanneurs conservent très peu d'argent comptant en caisse en dehors des heures d'ouverture normales. Bien que cette mesure de sécurité n'ait absolument aucun effet sur les vulnérabilités et ne prévienne en rien les vols à main armée, elle permet tout de même d'atténuer certaines conséquences en limitant les pertes financières. (On peut considérer comme un avantage secondaire un certain pouvoir de dissuasion, incitant les voleurs potentiels à aller voir ailleurs pour trouver des cibles plus lucratives.) On peut réduire considérablement la probabilité d'occurrence d'autres menaces, principalement les sinistres naturels, en évitant certains emplacements où divers problèmes sont susceptibles de survenir. Par exemple, on peut réduire les risques d'inondation en construisant sur un plateau surélevé, et les installations construites sur le Bouclier canadien subissent moins de tremblements de terre que celles qui sont construites près des principales lignes de faille.
- **Dissuasion.** Certaines mesures de protection, comme des panneaux de mise en garde bien en vue et de gros chiens de garde, visent à dissuader les agents de menaces délibérées qui songeraient à attaquer, réduisant par le fait même leurs intentions et, par conséquent, la probabilité d'occurrence. Comme les mesures d'évitement, les mécanismes de dissuasion ne visent pas directement les vulnérabilités; leurs répercussions sont donc prises en compte à la phase d'identification et d'évaluation des biens (dans le cas de certaines mesures d'évitement) et à la phase d'évaluation des menaces d'un projet d'EMR.[2]
- **Prévention.** Quelques mesures de prévention ciblent les agents de menaces délibérées afin de réduire la probabilité d'occurrence. Par exemple, la condamnation des voleurs peut limiter la capacité de ces derniers à commettre d'autres vols au moins pendant la durée de leur incarcération et, en théorie, la législation sur le contrôle des armes à feu devrait réduire les risques de vols à main armée. En règle générale, toutefois, la plupart des mesures préventives visent à réduire des vulnérabilités précises, afin de diminuer les risques de compromission si une menace venait à se concrétiser. La robustesse des mécanismes d'identification et d'authentification, par exemple, n'a pas un grand effet de dissuasion sur les pirates et est peu susceptible de réduire les probabilités d'attaque, mais peuvent tout de même empêcher la plupart des tentatives d'accès non autorisé à un système informatique, ce qui réduit les risques de compromission.
- **Détection.** La détection précoce des incidents peut permettre de contrer certaines vulnérabilités et favoriser une réaction rapide afin de contenir les dommages et de réduire la gravité des conséquences.
- **Réaction.** Seuls, les mécanismes de détection n'ont que peu d'effets sur la restriction des dommages causés par un incident. Toutefois, conjuguées à une réaction rapide,

[2] La question de l'incidence des mesures d'évitement sur les valeurs d'un bien est abordée à la section 4 de l'annexe B, alors que les effets des mécanismes d'évitement et de dissuasion sur la probabilité de réalisation des menaces sont examinés à la section 3 de l'annexe C.

l'ensemble des mesures de protection peuvent réduire considérablement les risques en diminuant les préjudices découlant d'une compromission.

- **Reprise.** Les mécanismes de reprise, par exemple les procédures de sauvegarde et l'entreposage hors site des données essentielles, permettent de contrer d'autres vulnérabilités et de faciliter la reprise rapide des activités normales, ce qui atténue encore la gravité des conséquences.

3.3 Mesures de protection : Répercussions sur les incidents

Comme il en est question ci-dessus, quelques mesures de protection facilitent l'élimination de certaines menaces, notamment les sinistres naturels, alors que d'autres dissuadent les agents de menaces délibérées. Bon nombre de mesures de sécurité visent à prévenir une compromission lorsqu'une menace se concrétise. Quelques-unes limitent les dommages subis en diminuant les valeurs des biens, et beaucoup d'autres atténuent les risques de préjudices grâce à des méthodes de détection précoce jumelées à des mécanismes de réaction et de reprise rapides. Les relations entre les différentes conséquences et les répercussions globales sur la probabilité d'occurrence d'une menace, la probabilité de compromission et la gravité des conséquences constituent les principaux critères d'évaluation de l'efficacité des mesures de protection.

- **Probabilité d'occurrence.** Lorsque c'est possible, le choix d'un emplacement où des incidents d'une catégorie particulière se sont rarement sinon jamais produits peut se révéler un moyen d'évitement très efficace pour réduire la probabilité d'éventuels problèmes. Par exemple, Vancouver a connu beaucoup moins de tempêtes de neige paralysantes que d'autres villes situées plus à l'Est, mais la côte Ouest est plus susceptible que le reste du pays de subir des tremblements de terre. Les probabilités relatives à différents endroits peuvent souvent être calculées assez précisément pour permettre une évaluation juste de l'efficacité des mesures de protection associées à bon nombre de méthodes d'évitement. Cependant, l'efficacité des mécanismes de dissuasion, comme des panneaux de mise en garde, pour réduire les risques d'incidents est généralement plus sujette à caution. Comme il est pratiquement impossible d'éviter ou de contrer toutes les menaces, d'autres approches doivent être adoptées pour créer un ensemble équilibré de mesures de protection qui se soutiennent mutuellement, afin d'atteindre un degré d'efficacité optimal.
- **Probabilité de compromission.** Des mesures de prévention plus rigoureuses sont davantage susceptibles de contrer une compromission en cas d'incident. Par exemple, une serrure à combinaison de qualité supérieure a plus de chances de prévenir l'accès clandestin à des biens sensibles qu'un cadenas à clé; il s'agit donc d'une mesure de protection plus efficace. Dans certains cas, la réduction effective de la probabilité de compromission peut être mesurée assez précisément et exprimée en termes très concrets, comme c'est le cas par exemple pour les algorithmes de chiffrement et les mots de passe de longueurs et de structures variées. En ce qui concerne d'autres mesures de protection, par exemple les initiatives de sensibilisation et de formation sur la sécurité, les incidences sont plus difficiles à cerner, et l'évaluation de leur efficacité est beaucoup plus subjective.

- **Gravité des conséquences.** Comme les mécanismes d'évitement, de dissuasion et de prévention sont rarement à toute épreuve, d'autres mesures de protection doivent normalement être mises en œuvre pour créer une stratégie de défense par couches, afin de limiter les dommages en cas de compromission, et de faciliter une reprise rapide et complète. Les systèmes de détection plus efficaces comme les alarmes anti-effraction, sont généralement plus difficiles à outrepasser, et donc plus susceptibles de révéler rapidement les activités non autorisées et de provoquer moins de fausses alertes. De la même manière, l'efficacité relative d'une réaction peut être mesurée en fonction de sa capacité à limiter ou à restreindre les préjudices découlant d'un incident. Par exemple, les édifices bien conçus peuvent généralement résister aux tremblements de terre, même les plus importants, sans subir de graves dommages. L'intégrité structurelle comme mesure de protection n'a aucune incidence sur la probabilité d'occurrence, mais peut réduire les préjudices auxquels on pourrait s'attendre.[3]

3.4 Tableau des incidences des mesures de protection

Les effets des mesures de protection sur les variables de risque et les incidents sont résumés dans le tableau D-1, Tableau des incidences des mesures de protection, selon les fonctions de sécurité qu'elles remplissent. Ces relations sont explorées plus en détail à l'annexe F, Phase des recommandations d'un projet d'EMR.

[3] En fait, l'intégrité structurelle peut empêcher les dommages de se produire, ce qui contribue à réduire la probabilité de compromission. Ainsi, cette mesure de protection peut remplir à la fois des fonctions de prévention et de réaction ou d'endiguement.

Fonctions de sécurité	Incidence des mesures de protection…						
	…sur les variables de risque				…sur les incidents		
	B_{Val}	M		V	O_{Prob}	C_{Prob}	C_{Grav}
		V	G				
Évitement[4]	⇓	↓			↓		⇓
		⇓			⇓		
Dissuasion		⇓			⇓		
Prévention[5]			↓	⇓	↓	⇓	
Détection				⇓			⇓
Réaction				⇓			⇓
Reprise				⇓			⇓

Légende

B_{Val} – Valeurs du bien. **M** – Menace. **P –**Probabilité de la menace.
G – Gravité de la menace (capacités de l'agent de menace). **V** – Vulnérabilité.
O_{Prob} – Probabilité d'occurrence. **C_{Prob} –** Probabilité de compromission.
C_{Grav} – Gravité des conséquences.
Incidence primaire – ⇓ Incidence secondaire – ↓

Tableau D-1 : Tableau des incidences des mesures de protection

4 Identification des vulnérabilités

4.1 Définition du terme « vulnérabilité »

4.1.1 Définition de la PGS

En vertu de la PGS, une vulnérabilité s'entend d'une « menace pouvant causer du tort en raison d'une sécurité insuffisante »[6]. Bien que cet énoncé définisse un des aspects important des vulnérabilités, notamment les répercussions défavorables de mesures de protection inadéquates, d'autres aspects doivent également être pris en compte.

4.1.2 Vulnérabilités en tant qu'attributs

On fait parfois fausse route en assimilant les vulnérabilités à des « faiblesses », parce qu'une vulnérabilité peut être une caractéristique souhaitable d'un bien. Par exemple, il n'est pas utile pour une galerie d'art de se procurer une toile précieuse pour ensuite l'enfermer dans le

4 La première ligne illustre l'incidence d'une réduction des valeurs des biens, principalement une diminution de la gravité des conséquences d'un incident compromettant assortie d'un déclin éventuel de la probabilité de réalisation de certaines menaces délibérées en raison d'un effet dissuasif. La deuxième ligne illustre l'incidence du choix du site pour éliminer certaines menaces, généralement des sinistres naturels, ainsi que le recul de la probabilité d'occurrence d'un incident qui en découle.

5 La plupart des mesures de prévention s'appliquent aux vulnérabilités afin de réduire la probabilité de compromission en cas d'incident, mais quelques-unes visent à restreindre les capacités des agents de menaces délibérées en réduisant soit la probabilité d'occurrence, soit la probabilité de compromission.

6 **Annexe B de la PGS, *Glossaire***.

coffre-fort. La toile doit être pouvoir être vue du public, même si cette accessibilité constitue aussi une vulnérabilité qui expose le bien à diverses menaces, comme le vol ou le vandalisme. Il convient donc mieux de définir les vulnérabilités comme des attributs, souhaitables ou non, qui rendent le bien plus susceptible d'être compromis. En outre, les vulnérabilités peuvent être des caractéristiques du bien lui-même, ou du milieu où il se trouve. Ainsi, le caractère mobile d'un ordinateur portatif, qui constitue une caractéristique souhaitable du bien, augmente les risques de vol, alors qu'une formation déficiente des employés de la compagnie d'électricité, qui constitue une caractéristique non souhaitable du milieu, peut accroître les risques de pannes d'électricité et la durée de ces dernières.

4.1.3 Effets des vulnérabilités

En règle générale, toutes les vulnérabilités peuvent contribuer aux risques de trois façons différentes. Tout d'abord, certains attributs augmentent la probabilité d'occurrence d'un incident. Par exemple, la visibilité des articles intéressants dans la vitrine d'une bijouterie peut encourager le vol. En deuxième lieu, certaines vulnérabilités augmentent le risque qu'un incident compromette un bien. Si on poursuit l'exemple précédent, la visibilité des biens précieux ne les rend pas nécessairement plus faciles à voler, mais un voleur est plus susceptible de réussir son coup si la vitrine n'est pas munie de barreaux ou de vitres incassables. Enfin, d'autres vulnérabilités font en sorte que les incidents causent davantage de dommages. Un dispositif antivol défectueux n'augmente pas en lui-même le risque d'une tentative de vol ou la probabilité de réussite d'une telle tentative, mais peut par contre retarder une réaction efficace, ce qui peut permettre au malfaiteur de causer davantage de dommages. Il va de soi que certaines vulnérabilités, comme une formation insuffisante, peuvent avoir un ou deux de ces effets secondaires, ou même les trois.

4.1.4 Vulnérabilités et efficacité des mesures de protection

Bien que certaines mesures de protection diminuent les risques par une manipulation des valeurs des biens ou des menaces plutôt qu'en atténuant les vulnérabilités, comme il en est question à la section 2.1 ci-dessus, la plupart des mesures de sécurité visent à corriger, directement ou indirectement, certaines vulnérabilités. Plus l'efficacité des mesures de protection augmente, plus les répercussions des vulnérabilités connexes ont tendance à diminuer. En d'autres mots, les vulnérabilités sont inversement proportionnelles à l'efficacité des mesures de protection, comme l'illustre la figure D-1. Cette relation est à la base des classes de vulnérabilités décrites plus loin.

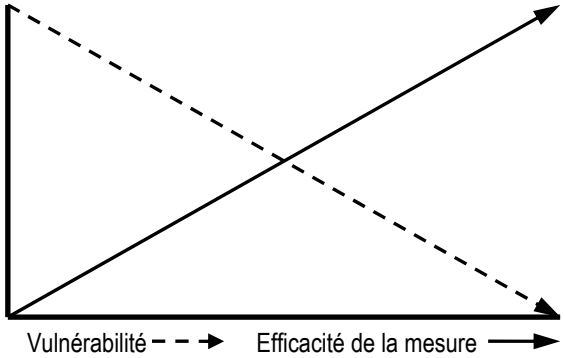

Figure D-1 : Vulnérabilités et efficacité des mesures de protection

4.1.5 Définition élargie

> ***Vulnérabilité*** *(vulnerability)* – attribut d'un bien, ou de l'environnement dans lequel il se trouve, qui augmente la probabilité d'un incident, la probabilité de compromission ou la gravité des conséquences. Les vulnérabilités sont inversement proportionnelles à l'efficacité des mesures de protection.
>
> Nouvelle définition

Aux fins de la méthodologie harmonisée d'EMR, la définition de base du terme « vulnérabilité » donnée dans la PGS est élargie, afin d'y intégrer les trois concepts présentés ci-dessus, soit (1) les vulnérabilités comme attributs des biens ou du milieu où ils se trouvent, (2) les effets des vulnérabilités sur la probabilité d'occurrence des incidents, les risques de compromission et l'ampleur des dommages qui en découlent, et (3) la relation inverse entre les vulnérabilités et l'efficacité des mesures de protection.

4.2 Classes de vulnérabilités

4.2.1 Généralités

Certaines mesures de protection, comme les mécanismes d'évitement et de dissuasion, ne touchent pas directement les vulnérabilités. Par contre, toutes les vulnérabilités, même celles qui constituent des attributs souhaitables, représentent une certaine faiblesse des mesures de sécurité qui y sont associées. Par exemple, un défaut de conception d'un élément de machinerie peut constituer une vulnérabilité susceptible d'augmenter le risque d'une panne majeure. Ce défaut peut être attribué à des mesures de protection inefficaces, par exemple un examen incomplet durant le processus de conception ou des essais marginaux inadéquats. Compte tenu de ce lien fondamental entre les vulnérabilités et les mesures de protection, les vulnérabilités peuvent être classées dans des catégories générales relatives aux exigences stratégiques de la PGS et des mesures de sécurité détaillées prescrites dans les normes opérationnelles de sécurité et les documents techniques connexes, décrites ci-dessous.

4.2.2 Programme de sécurité

Des rôles et des responsabilités en matière de sécurité mal définis, des ressources humaines et financières inadéquates et des politiques et procédures de sécurité incomplètes constituent des vulnérabilités particulièrement graves. Même si ces vulnérabilités n'augmentent pas la probabilité d'occurrence d'un incident quelconque, elles accroissent presque inévitablement le risque de compromission et la gravité des conséquences en cas d'incident, et peuvent avoir des effets désastreux sur la confidentialité, la disponibilité et l'intégrité.

4.2.3 Partage de l'information et des biens

Des ententes inadéquates en matière de partage de l'information, des installations et de l'infrastructure de TI peuvent donner lieu à bon nombre de vulnérabilités touchant à la fois la probabilité de compromission et la gravité des conséquences, en plus d'avoir également une incidence néfaste sur la confidentialité, la disponibilité et l'intégrité.

4.2.4 Sécurité à l'extérieur du Canada

Les risques pour la sécurité varient considérablement d'une région du monde à l'autre; des évaluations périodiques sont donc nécessaires pour éliminer d'éventuelles vulnérabilités susceptibles d'exposer les employés et les biens à une probabilité accrue de compromission et de conséquences graves. Encore une fois, les trois valeurs des biens (confidentialité, disponibilité

et intégrité) peuvent être touchées. Dans le cas des restrictions relatives aux déplacements, des évaluations mal éclairées pourraient également inciter les Canadiens à visiter des endroits où la probabilité de réalisation de certains risques est plus élevée qu'ailleurs.

4.2.5 Passation de marchés

Le manque de connaissance des critères de sécurité de la passation de marchés et des procédures connexes relatives aux Listes de vérification des exigences relatives à la sécurité (LVERS)[7] et aux attestations de sécurité des installations peut accroître le risque de compromission, particulièrement le risque de divulgation non autorisée d'information classifiée ou protégée.

4.2.6 Sensibilisation à la sécurité et formation

Des initiatives inadéquates en matière de sensibilisation à la sécurité et de formation font partie des vulnérabilités les plus graves, parce qu'elles peuvent mettre en péril pratiquement tous les biens, accroître la probabilité d'occurrence d'incidents, ainsi que la probabilité de compromission et la gravité des conséquences, ce qui a des répercussions sur la confidentialité, la disponibilité et l'intégrité.

4.2.7 Identification des biens

Une classification et une identification inadéquates des biens peuvent donner lieu à de graves vulnérabilités menant à une gestion des risques déficiente et à une application inadéquate d'autres mesures de protection, ce qui accroît la probabilité de compromission et la gravité des conséquences pour la confidentialité, la disponibilité ou l'intégrité, selon les valeurs des biens touchées.

4.2.8 Gestion des risques liés à la sécurité

Comme la mise en œuvre de normes de sécurité de base et la gestion continue des risques constituent les deux fondements pour la sélection de toutes les autres mesures de protection, toute défaillance dans la gestion des risques liés à la sécurité pourrait avoir un effet de cascade et introduire beaucoup d'autres vulnérabilités, augmenter la probabilité d'occurrence des incidents et accroître la probabilité de compromission et la gravité des conséquences, ce qui toucherait la confidentialité, la disponibilité et l'intégrité.

4.2.9 Limites d'accès

Des restrictions d'accès inadéquates peuvent accroître à la fois la probabilité de compromission, et la gravité des conséquences. Le principe de l'accès sélectif s'applique principalement à la confidentialité, alors que les autres mesures de protection peuvent contribuer à la protection des trois valeurs des biens.

4.2.10 Filtrage de sécurité

Si le processus initial de filtrage est défaillant, la probabilité de compromission peut augmenter considérablement. Réciproquement, les vulnérabilités découlant de procédures inadéquates d'examen, de révocation et de diffusion peuvent contribuer à accroître la gravité des conséquences. Des attestations de sécurité et des autorisations d'accès aux sites bâclées ont

7 Le formulaire TBS/SCT 350-103 (2004/12) se trouve au site suivant : http://www.tbs-sct.gc.ca/tbsf-fsct/350-103_f.asp.

tendance à mettre en péril la confidentialité, alors que des vérifications de la fiabilité peu rigoureuses peuvent menacer les trois valeurs des biens.

4.2.11 Protection des employés

Les vulnérabilités associées à des mesures inefficaces de protection des employés peuvent augmenter le risque et la gravité des préjudices corporels et psychologiques et soulever des préoccupations graves concernant la disponibilité.

4.2.12 Sécurité matérielle

Les mesures de sécurité matérielle remplissent une vaste gamme de fonctions de sécurité; les répercussions de toute vulnérabilité connexe sur la probabilité d'occurrence, la probabilité de compromission et la gravité des conséquences varient donc considérablement, tout comme les valeurs des biens touchées. Certaines mesures, comme le choix du site, constituent principalement des mécanismes d'évitement; quand on choisit un emplacement où les menaces sont moins susceptibles de se produire, les vulnérabilités éventuelles n'augmentent pas le risque de réalisation des menaces. Outre les signes extérieurs, qui sont le plus souvent de nature dissuasive, la plupart des mesures de sécurité périphérique visent à prévenir la compromission des biens par certaines menaces ou à déceler ces dernières le plus tôt possible afin de limiter les dégâts. Toute vulnérabilité relative à la sécurité matérielle est susceptible d'accroître la probabilité de compromission ou la gravité des conséquences, et d'avoir des répercussions défavorables sur la confidentialité, la disponibilité et l'intégrité. D'autres vulnérabilités liées aux contrôles de l'accès, à la gestion des installations, à l'entreposage sécurisé et au transport et à la transmission, à quelques exceptions près, touchent les trois valeurs des biens, mais la principale répercussion sur les risques consiste en une augmentation de la probabilité de compromission, puisqu'il s'agit essentiellement de mécanismes de prévention. Les mesures de destruction sont conçues pour prévenir la divulgation non autorisée; les vulnérabilités connexes concernent donc généralement la confidentialité, ainsi qu'une probabilité accrue de compromission.

4.2.13 Sécurité des TI

Comme les mesures de sécurité matérielle, les mesures de protection des TI remplissent différentes fonctions de sécurité, notamment la prévention, la détection, la réaction et la reprise. Par conséquent, toute vulnérabilité relative à la sécurité des TI peut accroître le risque de compromission ou la gravité des conséquences. Certaines mesures de sécurité des TI, par exemple les contrôles de gestion, touchent les trois valeurs des biens, alors que d'autres sont plus ciblées. La plupart des mesures de protection techniques sont de nature préventive, de sorte qu'une faiblesse augmente la probabilité de compromission; toutefois, des mesures de protection contre le code malveillant peuvent également comporter des fonctions de détection et de réaction, de sorte qu'une défaillance peut aussi aggraver les conséquences. Comme la détection des intrusions et la sauvegarde/reprise constituent respectivement des mécanismes de détection et de reprise, les vulnérabilités qui y sont associées sont susceptibles d'aggraver les conséquences. Certaines mesures de protection techniques, par exemple l'infrastructure à clé publique (ICP), peuvent protéger les trois valeurs des biens, alors que d'autres n'en touchent qu'une ou deux. Par exemple, la sécurité des émissions vise strictement la confidentialité, alors que les procédures de sauvegarde et de reprise visent à protéger la disponibilité. Enfin, toute vulnérabilité liée aux mesures de protection opérationnelles est susceptible d'accroître la probabilité de compromission ou la gravité des conséquences. La plupart ont des répercussions

sur les trois valeurs des biens, mais la planification de la capacité, la protection de l'environnement, le conditionnement de l'énergie et la sauvegarde sont fondamentalement des questions de disponibilité.

4.2.14 Sécurité dans les situations d'urgence

Si des niveaux de préparation et des procédures de sécurité connexes ne sont pas clairement établis, la réaction dans les situations d'urgence et de menace accrue peut être trop lente ou incomplète, ce qui risque d'aggraver considérablement les conséquences. Dans certains cas, lorsque la menace est précédée d'un avertissement, ces vulnérabilités peuvent également accroître le risque de compromission. Bien que certaines situations d'urgence puissent avoir des répercussions sur la confidentialité ou l'intégrité, la plupart entraînent la destruction de biens et l'interruption des services, deux problèmes relatifs à la disponibilité.

4.2.15 Planification de la continuité des activités

Toute faiblesse relative à la planification de la continuité des activités est susceptible de retarder la reprise des services essentiels dans l'éventualité d'une perte, ce qui aggrave les conséquences et peut constituer un problème grave de disponibilité.

4.2.16 Enquêtes sur les incidents

Les vulnérabilités découlant de procédures inefficaces d'enquête et de présentation de rapports peuvent augmenter la probabilité d'une compromission accrue si les causes principales ne sont pas évaluées correctement. De la même manière, les préjudices qui découlent des incidents pourraient augmenter et avoir des conséquences fâcheuses sur la confidentialité, la disponibilité ou l'intégrité, selon la nature de l'incident de sécurité.

4.2.17 Sanctions

Des sanctions officielles peuvent dissuader les récidivistes; l'absence de sanctions peut donc augmenter la probabilité d'autres infractions. De la même manière, si on néglige de congédier ou de muter les auteurs de méfaits graves à titre préventif, on peut les inciter à commettre d'autres infractions, et la probabilité de récurrence augmente, ce qui risque de compromettre la confidentialité, la disponibilité ou l'intégrité, selon la nature des infractions à la sécurité.

4.3 Sources des données sur les vulnérabilités

4.3.1 Partage de l'information

Les données sur les vulnérabilités sont souvent plus difficiles à recueillir et à évaluer que les données sur les autres variables de risque, car bon nombre d'organismes sont réticents à admettre des défaillances ou des faiblesses en ce qui a trait à la sécurité de leurs produits, de leurs programmes ou de leurs installations par crainte d'être blâmé ou de faire l'objet de poursuites devant les tribunaux. C'est pourquoi, comme il en est question à la section 2 de l'annexe A, portant sur la phase de préparation, l'engagement de la haute direction envers le processus d'EMR est essentiel pour surmonter ces obstacles et promouvoir le partage d'information pour le bien de l'ensemble de l'organisme.

4.3.2 Ressources ministérielles

Une fois ces questions résolues, toutefois, les gestionnaires ministériels et les responsables de la sécurité ont un grand rôle à jouer. Une bonne compréhension des processus opérationnels pertinents peut faciliter le repérage de certaines vulnérabilités, particulièrement en ce qui a trait à la sécurité globale. Un examen rigoureux des documents de conception, des schémas et des plans d'étage peut aussi procurer des renseignements précieux. Les gestionnaires des installations et les administrateurs des systèmes connaissent les problèmes qui se sont produits dans le passé et savent donc quelles faiblesses au plan de la sécurité ont exposé les biens ou les employés à des préjudices. Les responsables ministériels de la sécurité comprennent la plupart des mesures de protection mises en œuvre à ce jour, et connaissent bon nombre des lacunes qui leurs sont inhérentes. Dans le cas des systèmes de TI en particulier, des essais et des évaluations axés sur la sécurité peuvent révéler beaucoup de failles (mais pas toutes). Les vérifications internes et les examens sont souvent axés sur la pertinence des contrôles de gestion. Les responsables des finances, des ressources humaines et de la santé et sécurité au travail peuvent également fournir des renseignements sur les vulnérabilités propres aux systèmes financiers et aux employés, respectivement.

4.3.3 Ressources externes

Certains ministères responsables en matière de sécurité offrent des services-conseils complets et une orientation sur toute une gamme de mesures de protection, et sur au moins certaines des vulnérabilités qui y sont associées. Plusieurs associations professionnelles explorent différents aspects de la sécurité, offrent des évaluations de différentes mesures de protection et des vulnérabilités connexes. Bon nombre de périodiques publient des articles portant sur des produits de sécurité et commentant leur efficacité. Un certain nombre de sites Web offrent également de l'information à jour sur les vulnérabilités techniques associées à différents systèmes et produits de TI.

4.3.4 Résumé

L'appendice D-1 dresse la liste des diverses sources éventuelles de données sur les vulnérabilités, ainsi que le type d'information qu'elles peuvent fournir à l'équipe de l'EMR.

4.4 Techniques de collecte des données

Comme pour le processus d'identification des biens décrits à la section 2 de l'annexe B, la première étape d'une collecte de données sur les vulnérabilités consiste en un examen minutieux de la documentation pertinente. Parmi les documents intéressants, mentionnons les plans d'activités et les politiques du ministère en matière de sécurité, ainsi que les documents plus spécifiques directement liés à l'objet du projet d'EMR, y compris les manuels d'installation et les guides d'utilisation, dont certains sont énumérés à l'appendice D-1. Les constatations issues de cette recherche doivent être confirmées par des entrevues avec les responsables compétents en matière de programmes, de projets, de gestion des installations, de TI et de sécurité, selon la nature de l'évaluation. Bien que la plupart des renseignements recueillis soient recevables tels quels, il est généralement préférable de corroborer les résultats au moyen d'inspections sur place et d'essais de sécurité. Une vérification et une validation indépendantes pourraient se révéler utiles dans le cas des biens particulièrement sensibles exposés à un risque élevé, afin de garantir l'intégralité et l'objectivité de l'évaluation des vulnérabilités. Enfin, la *Méthodologie harmonisée*

d'EMR comprend une liste considérable de vulnérabilités (voir appendice D-2) qui peut servir d'aide-mémoire durant le processus d'identification des vulnérabilités.

4.5 Liste des vulnérabilités

4.5.1 Structure

La liste des vulnérabilités de l'appendice D-2 se présente sous la forme d'une structure hiérarchisée, qui ressemble à celle des listes des biens et des menaces présentées aux appendices B-2 et C-2 respectivement. À partir des 16 classes de vulnérabilités décrites à la section 4.2, la liste se divise pour définir plus en détail des groupes de vulnérabilités et certaines vulnérabilités distinctes. Les niveaux des embranchements sont définis ci-dessous, et la structure réelle est illustrée à la figure D-2 :

- **Classe de vulnérabilités.** Groupe générique de vulnérabilités axé sur les exigences stratégiques générales en matière de sécurité énoncées dans la PGS et dans les documents connexes.
- **Groupe de vulnérabilités.** Subdivision des classes de vulnérabilités, visant à regrouper toutes les vulnérabilités associées à un groupe connexe de mesures de sécurité.
- **Vulnérabilité spécifique.** Faille ou faiblesse réelle liée à une mesure de protection spécifique, susceptible de compromettre la sécurité des employés, des biens ou de la prestation des services.

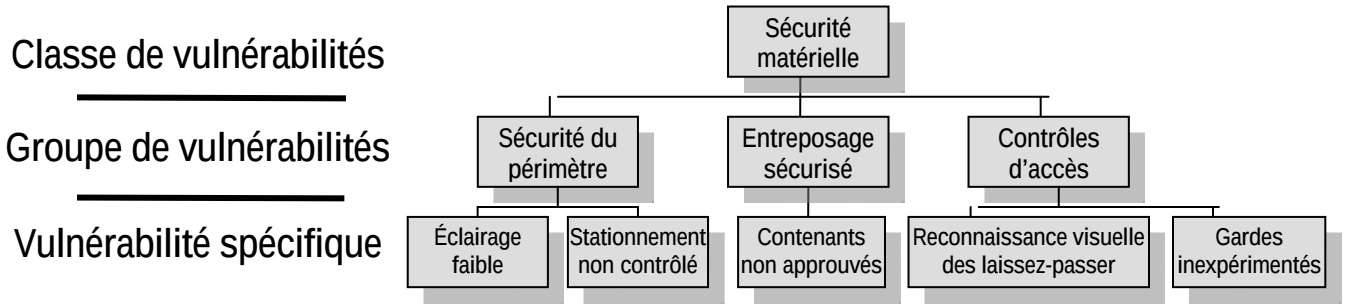

Figure D-2 : Structure hiérarchique de la liste des vulnérabilités

4.5.2 Avantages

Comme les listes des biens et des menaces, la liste des vulnérabilités organisée selon une structure hiérarchisée présente plusieurs avantages importants pour la réalisation d'un projet d'EMR :

- **Cohérence.** Le recours à des structures et à des définitions communes des données pour l'identification des vulnérabilités facilite la communication à l'intérieur d'un même projet d'EMR et entre projets, afin d'atteindre des résultats cohérents qui peuvent être reproduits par d'autres spécialistes évaluant des vulnérabilités identiques ou semblables. Il favorise également l'interopérabilité pour le partage entre organismes des données sur les vulnérabilités.
- **Exhaustivité.** Les vulnérabilités importantes sont moins susceptibles d'être omises lorsque les équipes chargées de l'EMR utilisent des listes exhaustives.

- **Flexibilité et extensibilité.** La liste des vulnérabilités offre moins d'avantages que les listes des biens et des menaces correspondantes en termes de souplesse et d'extensibilité, puisque la plupart des faiblesses doivent être évaluées à un degré de détail le moins élevé possible. Par contre, des embranchements entiers de la structure arborescente peuvent être ignorés si la classe de vulnérabilités ne fait pas partie de la portée de l'évaluation. Par exemple, les vulnérabilités relatives à la protection des employés peuvent être exclues dans les situations où le personnel ne constitue pas un problème.
- **Documentation à jour.** La liste des vulnérabilités peut facilement être mise à jour lorsque de nouvelles vulnérabilités sont recensées. En outre, compte tenu du regroupement logique des vulnérabilités similaires, il est beaucoup plus simple de classer les nouveaux problèmes.

4.5.3 Mise en garde

Encore une fois, comme c'est le cas pour les listes des biens et des menaces, la liste des vulnérabilités doit être utilisée avec prudence. Elle n'est pas et ne peut pas être exhaustive, puisque de nouvelles vulnérabilités, particulièrement dans le domaine des TI, sont découvertes régulièrement, en partie à cause de l'évolution rapide des technologies et des capacités des agents de menace. **L'appendice D-2 doit donc être utilisé comme un aide-mémoire et un guide pour faciliter l'organisation et la structure de la collecte et du traitement des données sur les vulnérabilités pertinentes, et non comme une liste de vérification à respecter aveuglément.**

5 Analyse de l'incidence des vulnérabilités

5.1 Paramètres des vulnérabilités

Comme il est indiqué à la section 4.1 ci-dessus, toutes les vulnérabilités peuvent contribuer au risque de trois manières différentes. Quelques vulnérabilités, par exemple un emplacement défavorable ou la visibilité de biens de grande valeur, peuvent accroître la probabilité d'occurrence d'un incident. Par conséquent, les vulnérabilités de cette nature sont généralement prises en compte dans l'évaluation de la probabilité dans le cadre de la phase d'évaluation des menaces d'un projet d'EMR, dont il est question à la section 3 de l'annexe C. Les autres incidences potentielles des vulnérabilités, soit une augmentation de la probabilité de compromission ou une aggravation des conséquences, sont à la base de la définition de paramètres qui permettent l'analyse comparative des différentes vulnérabilités exposant divers biens à des préjudices.

5.2 Probabilité de compromission

5.2.1 Généralités

Des mesures de prévention efficaces réduisent la probabilité qu'un incident compromette un bien. Toute vulnérabilité ou défaillance associée à ces mesures de protection a l'effet opposé, c'est-à-dire qu'elle augmente le risque de divulgation, de destruction, de suppression, de modification, d'interruption d'accès ou d'utilisation non autorisées de biens, selon la nature de la menace.

5.2.2 Critères d'évaluation de base

Parmi les facteurs importants à prendre en compte dans l'évaluation de l'incidence des vulnérabilités liées à des mesures de prévention inadéquates ou inefficaces, mentionnons les suivants :

- **Probabilité de prévention.** Si aucune mesure de prévention n'est en place, ou si les mesures sont généralement inefficaces, la probabilité de compromission qui en découle est élevée, s'approchant même de la certitude absolue dans la pire éventualité. Des mécanismes de prévention moyennement efficaces contrent au moins une partie des menaces, tout en permettant aux autres de causer des préjudices, de sorte que la probabilité de compromission est jugée moyenne. Des mesures de protection très efficaces préviennent les dommages dans la plupart des cas, ce qui réduit la probabilité de compromission à un niveau faible.
- **Facilité d'exploitation.** Les vulnérabilités qui exposent les biens à des menaces délibérées peuvent être cotées en fonction de leur facilité d'exploitation. Les vulnérabilités dont il est facile de profiter, qu'on peut exploiter avec peu de connaissances, de compétences ou de ressources spécialisées, sont particulièrement dangereuses parce que la probabilité de compromission qui y est associée est élevée. D'autres vulnérabilités dont l'exploitation exige quelques connaissances, compétences ou ressources sont plus susceptibles d'échapper à certaines menaces; la probabilité de compromission s'établit alors à un niveau moyen. Enfin, les vulnérabilités très complexes qui sont difficiles à comprendre ou dont l'exploitation exige des compétences et des ressources particulières ont une incidence faible sur la probabilité de compromission. Aux fins d'analyse dans le cadre de l'évaluation des vulnérabilités en fonction de ce paramètre, les connaissances requises pour circonvenir à une mesure de protection peuvent provenir d'une formation formelle, d'un encadrement ou de l'expérience pratique. Si, par exemple, un attaquant doit avoir un diplôme universitaire dans un domaine d'études spécialisé pour comprendre une vulnérabilité, les répercussions sur la probabilité de compromission sont vraisemblablement faibles. Par compétence, on entend une certaine dextérité manuelle ou des aptitudes intellectuelles particulières, une certaine acuité auditive ou visuelle ou d'autres caractéristiques individuelles des agents de menace potentiels. Quant aux ressources, il peut s'agir d'un soutien financier ou de l'accès à des outils d'attaque spécialisés, comme des superordinateurs pour déchiffrer des codes de haut niveau.

- **Attributs pertinents des biens.** Certaines lacunes des mesures de prévention sont clairement liées à divers attributs des biens ou du milieu où ils se trouvent. Par exemple, un accès facile peut favoriser de nombreuses menaces, chacune assortie d'une augmentation de la probabilité de compromission correspondante. Les articles fragiles sont plus susceptibles d'être endommagés. Les mécanismes complexes sont plus susceptibles de faillir. Les petits objets portatifs sont plus faciles à dissimuler et à emporter. La probabilité de compromission associée à des biens moins accessibles, plus robustes, plus simples et solidement fixés a tendance à diminuer.
- **Sensibilisation/formation des employés.** Des employés mal formés et ne connaissant pas leurs responsabilités sont moins susceptibles de prévenir beaucoup de menaces délibérées et accidentelles, ce qui fait augmenter la probabilité de compromission. Par contre, des employés bien informés, correctement formés et hautement motivés sont plus susceptibles de prévenir les menaces entraînant une compromission des biens.

5.2.3 Incidence sur la probabilité de compromission

Pour chaque vulnérabilité ayant des répercussions sur les biens inclus dans la portée de l'évaluation, il faut déterminer l'incidence de la probabilité de compromission en fonction de l'efficacité relative des mécanismes de prévention connexes, de la facilité d'exploitation, des effets potentiels des attributs défavorables des biens et de l'ampleur de la sensibilisation et de la formation des employés. Il convient d'affecter une cote Élevée, Moyenne ou Faible à la probabilité de compromission en fonction du tableau D-2, *Incidence des vulnérabilités sur la prévention*, ou encore la mention « sans objet » si la vulnérabilité ne concerne que les mesures de détection, de réponse ou de reprise.

Efficacité des mesures de protection	Vulnérabilités connexes	Probabilité de compromission
Aucune mesure de protection Mesure inefficace en grande partie Probabilité de compromission > 75 %	Facilement exploitables Besoin de peu de connaissances/ compétences/ressources Biens hautement accessibles Biens très complexes/fragiles/portables Employés mal informés/formés	Élevée
Mesure modérément efficace Probabilité de compromission 25-75 %	Pas facilement exploitables Besoin de certaines connaissances/ compétences/ressources Biens modérément accessibles Biens modérément complexes/fragiles/portables Employés modérément informés/formés	Moyenne
Mesure très efficace Probabilité de compromission < 25 % (mesure remplissant uniquement des fonctions de détection, de réaction ou de reprise)	Difficiles à exploiter Besoin de très bonnes connaissances/ compétences/ressources Accès aux biens rigoureusement contrôlé Biens très simples/robustes/statiques Employés bien informés/formés	Faible (sans objet)

Tableau D-2 : Incidence des vulnérabilités sur la probabilité de compromission (prévention)

5.3 Gravité des conséquences

5.3.1 Généralités

Des mesures efficaces de détection, de réaction et de reprise réduisent les dommages découlant d'un incident compromettant. Toute vulnérabilité ou faiblesse associée à ces mesures de protection ont l'effet opposé, c'est-à-dire qu'elle accroît, soit en importance, soit en durée, la gravité de la divulgation, de la destruction, de la suppression, de la modification, de l'interruption ou de l'utilisation non autorisées des biens.

5.3.2 Critères d'évaluation de base

Parmi les facteurs importants à prendre en considération dans l'évaluation de l'incidence des vulnérabilités susceptibles d'accroître la gravité de la compromission, mentionnons :

- **Détection.** L'efficacité d'un mécanisme de détection, quel qu'il soit, dépend généralement de deux attributs, soit le degré de certitude de la détection de certains incidents et la promptitude avec laquelle le mécanisme permet de réagir. Les faiblesses et vulnérabilités associées à ces mesures de protection peuvent aggraver la compromission en faisant en sorte que celle-ci demeure inaperçue et non vérifiée. En l'absence de mesures de protection, ou si les mesures de détection ne sont pas suffisamment efficaces, l'incidence sur la gravité des conséquences est élevée. Lorsqu'il existe une probabilité significative que les incidents soient décelés après un

certain temps, l'incidence est alors jugée moyenne. Si une détection immédiate est presque certaine, la vulnérabilité a alors une incidence faible.

- **Réaction.** Lorsqu'un incident compromettant est détecté, des mécanismes de réaction peuvent être mis en branle pour limiter ou contenir les préjudices qui en découlent. Par exemple, des détecteurs de chaleur ou de fumée (deux dispositifs de détection) peuvent déclencher l'activation d'un système d'extincteurs (mesure d'extinction des incendies). Toute faiblesse ou vulnérabilité associée à ces mesures de sécurité peut aggraver la compromission et avoir une incidence allant de faible (dommages rigoureusement contenus) à élevée (faible degré d'intervention pour limiter les préjudices).
- **Reprise.** Comme pour les mécanismes de détection, l'efficacité des mesures de reprise peut être évaluée selon deux critères, soit le délai avant le rétablissement des biens ou des services touchés, et le degré de rétablissement réalisé. Des mesures de protection efficaces permettent généralement un rétablissement rapide des opérations normales, alors que les vulnérabilités connexes peuvent introduire des délais ou empêcher le rétablissement complet, ce qui accroît la gravité de la compromission. Par exemple, dans le contexte des TI, un site de secours entièrement équipé et mis à l'essai peut permettre la reprise presque immédiate de la totalité des services à la suite d'une interruption, de sorte que l'incidence sur la gravité des conséquences est jugée faible. Au contraire, l'absence totale de données de sauvegarde peut tuer tout espoir de reprise, de sorte que l'incidence d'une telle vulnérabilité sur la gravité de la compromission est jugée élevée.
- **Attributs pertinents des biens.** Encore une fois, certaines vulnérabilités associées aux mécanismes de détection, de réaction et de reprise sont liés à des attributs des biens ou du milieu où ils se trouvent. La complexité des biens constitue une des principales préoccupations, parce qu'il peut être plus difficile de déceler une compromission lorsque l'équipement et les systèmes de TI sont complexes. Ainsi, le repérage d'une erreur, même accidentelle, parmi les millions de lignes de code d'un système d'exploitation, constitue un défi de taille. Les mesures de réaction et de reprise appropriées peuvent être plus difficiles à évaluer, et leur mise en œuvre plus longue, de sorte que les préjudices qui en découlent peuvent être plus difficiles à contenir, et que le rétablissement des services normaux peut devenir problématique. Selon le degré de complexité, l'incidence sur la gravité de la compromission peut aller de faible à élevée. Les effets de la fragilité ou de toute autre faiblesse relative à l'intégrité structurelle, peuvent être difficiles à maîtriser et, dans la pire éventualité, provoquer des dommages si importants que toute reprise réaliste est presque impossible.
- **Sensibilisation/formation des employés.** Sans une formation et une sensibilisation adéquates, même un employé consciencieux est moins en mesure de reconnaître et de réagir aux incidents, ce qui risque d'accroître les préjudices découlant d'une compromission. Le personnel bien informé à qui on a offert une formation appropriée pourra déceler bon nombre de problèmes et prendre les mesures qui s'imposent pour limiter les dommages et favoriser une reprise rapide.

5.3.3 Incidence sur la gravité des conséquences

Pour chaque vulnérabilité constituant un risque pour les biens inclus dans la portée de l'évaluation, il faut déterminer l'incidence sur la gravité de la compromission en fonction de l'efficacité relative des mécanismes connexes de détection, de réaction et de reprise, des effets potentiels des attributs défavorables des biens et de l'ampleur de la sensibilisation et de la formation des employés. Il convient d'affecter une cote Élevée, Moyenne ou Faible à la gravité des conséquences en fonction du tableau D-3, *Incidence des vulnérabilités sur la détection, la réaction ou la reprise*, ou encore la mention « sans objet » si la vulnérabilité ne concerne que les mesures de prévention.

Efficacité de la mesure de protection	Vulnérabilités connexes	Gravité des conséquences
Aucune mesure de protection Mesure en grande partie inefficace Biens exposés à des préjudices importants	Détection improbable des compromissions Dommages difficiles à contenir Délais de reprise prolongés/Niveaux de service faibles Biens très complexes/fragiles Employés mal informés/formés	Élevée
Mesure modérément efficace Biens exposés à des préjudices modérés	Compromissions probablement détectées au fil du temps Dommages partiellement contenus Délais de reprise/Niveaux de service modérés Biens relativement complexes/fragiles Employés modérément informés/formés	Moyenne
Mesure très efficace Biens exposés à des préjudices limités (Mesure remplissant uniquement une fonction de prévention)	Compromissions presque certainement détectées rapidement Dommages rigoureusement contenus Reprise rapide et complète Biens très simples/robustes Employés bien informés/formés	Faible (sans objet)

Tableau D-3 : Incidence des vulnérabilités sur la gravité des conséquences (détection, réaction ou reprise)

6 Évaluation des vulnérabilités

6.1 Niveaux de vulnérabilités

6.1.1 Évaluation de base des vulnérabilités

Lorsque l'incidence d'une vulnérabilité sur la probabilité de compromission et la gravité des conséquences a été déterminée à l'aide des tableaux D-2 et D-3 respectivement, il suffit d'entrer ces deux valeurs dans le tableau D-4 pour obtenir une cote globale, qui peut aller de Très faible à Très élevée, pour chaque vulnérabilité exposant les biens inclus dans la portée de l'évaluation aux menaces identifiées à la phase d'évaluation des menaces.

Incidence sur la gravité des conséquences (détection, réaction et reprise)	Incidence sur la probabilité de compromission		
	Faible (s.o.)	**Moyenne**	**Élevée**
Élevée	Moyenne	Élevée	Très élevée
Moyenne	Faible	Moyenne	Élevée
Faible (s.o.)	Très faible	Faible	Moyenne

Tableau D-4 : Évaluation de base des vulnérabilités

6.1.2 Vulnérabilités connexes

Malheureusement, l'évaluation de base des vulnérabilités a ses limites. Une même faiblesse touchant à la fois la probabilité de compromission et la gravité des conséquences peut se voir attribuer n'importe laquelle des cinq cotes selon ses répercussions réelles ou prévues, alors qu'une vulnérabilité relative à une seule fonction de protection (prévention, ou détection, réaction et reprise), quelle que soit la gravité de ses conséquences, obtiendrait une cote maximale « moyenne » au tableau D-4. Dans certains cas, il ne s'agit pas d'un problème grave parce que, par exemple, des mécanismes robustes de détection, de réaction et de reprise peuvent souvent compenser des mesures de prévention inadéquates ou inefficaces. De la même manière, des mesures de détection, de réaction et de reprise moins efficaces peuvent être tout à fait acceptables lorsque les mesures préventives connexes sont particulièrement robustes. Le véritable problème survient lorsqu'il existe des faiblesses différentes mais complémentaires liées à la fois à la prévention, et à la détection, à la réaction et à la reprise. Comme c'est fréquemment le cas, l'évaluation de base des vulnérabilités doit être élargie afin d'examiner les effets de cascade des vulnérabilités connexes.

6.1.3 Évaluation étendue de la vulnérabilité

Pour contrer ce phénomène important, une évaluation étendue de la vulnérabilité devrait être appliquée à toutes les vulnérabilités qui sont assorties d'une cote Sans objet pour la prévention ou la détection, la réaction et la reprise. Dans chaque cas, il faudrait identifier toute vulnérabilité connexe touchant la dimension Sans objet, tant pour l'incidence sur la probabilité de compromission que pour l'incidence sur la gravité des conséquences, afin d'en calculer leur incidence combinée comme suit :

- **Scénario simple.** Souvent, l'une des vulnérabilités connexes aura des répercussions uniquement sur la probabilité de compromission (mesure de prévention faible), tandis que l'autre touchera uniquement la gravité des conséquences (mécanismes de détection, de réaction ou de reprise inadéquats). L'évaluation étendue des vulnérabilités consiste simplement à entrer les deux valeurs dans le tableau D-4.
- **Scénario combiné.** À l'occasion, ce processus simple peut être compliqué lorsque la vulnérabilité connexe touche à la fois la probabilité de compromission et la gravité des conséquences, donnant lieu à deux cotes pour l'une de ces valeurs, une pour chacune des vulnérabilités connexes. Lorsque les cotes sont identiques (soit Faible, Moyenne ou Élevée), le calcul de leur incidence combinée est essentiellement la

même que dans le scénario simple ci-dessus. Lorsque les deux valeurs diffèrent, cependant, il faudrait en sélectionner une pour l'évaluation étendue des vulnérabilités en s'appuyant sur la justification suivante :

- si la vulnérabilité la plus grave est compensée par la mesure de protection la plus efficace avec la cote de vulnérabilité la plus faible, alors on utilise la valeur la plus faible;
- si la vulnérabilité la plus grave amoindrit l'efficacité de la mesure de protection la moins vulnérable, alors on utilise la valeur la plus élevée.

6.1.4 Exemples d'évaluation

Voici deux exemples concrets servant à illustrer l'évaluation étendue des vulnérabilités :

- **Scénario simple.** Une serrure peu coûteuse sur la porte d'un entrepôt n'aura que peu d'effet sur la prévention de l'accès non autorisé et du vol. Par contre, les faiblesses du moyen de prévention n'ont pas d'effets directs sur la gravité des conséquences, puisque la serrure ne remplit aucune fonction de détection, de réaction ou de reprise. Par conséquent, en vertu de l'évaluation de base des vulnérabilités, cette faiblesse justifierait simplement une cote Moyenne. Si en plus il n'y a pas de garde ou d'alarme anti-effraction pour détecter les accès non autorisés, l'absence d'un mécanisme de détection serait cotée Élevée à cause de son incidence sur la gravité des conséquences, alors que la cote globale calculée à l'aide du tableau D-4 ne serait que Moyenne. Toutefois, si on tient compte de l'effet combiné des deux vulnérabilités et qu'on applique de nouveau l'évaluation de base de vulnérabilités au tableau D-4, on obtient une cote globale Très élevée, ce qui constitue une conclusion beaucoup plus réaliste.
- **Scénario combiné.** Si l'entrepôt aux serrures inefficaces (ce qui représente une vulnérabilité moyenne selon l'évaluation de base des vulnérabilités effectuée plus haut) se voyait doté d'un garde de sécurité bien formé, la vulnérabilité connexe pourrait être cotée Faible si le garde constitue une mesure de prévention moyennement efficace et des capacités de détection et de réaction très efficaces. Même si on a deux valeurs différentes pour l'incidence sur la probabilité de compromission (Élevée pour la serrure et Moyenne pour le garde), on doit n'en sélectionner qu'une seule pour l'évaluation étendue des vulnérabilités. S'il est improbable qu'une serrure inadéquate nuise à la capacité du garde d'exercer des fonctions de prévention modérément efficaces, la plus faible valeur (Moyenne) pour l'incidence sur la probabilité de compromission devrait être utilisée. Si, toutefois, il y a possibilité que la serrure soit exploitée pour éviter l'intervention du garde, ce qui nuirait à l'efficacité de ce dernier, alors il faudrait utiliser la valeur plus élevée (Élevée) pour l'incidence sur la probabilité de compromission. Ainsi, la cote résultant de l'évaluation étendue des vulnérabilités serait soit Faible, soit Moyenne pour les vulnérabilités connexes, selon leur interaction la plus probable.

6.2 Application pratique

6.2.1 Généralités

Pour mettre en application l'évaluation étendue des vulnérabilités et faciliter le calcul du risque résiduel à la deuxième étape de la phase d'évaluation des risques d'un projet d'EMR, il faut déterminer quels biens et quelles valeurs des biens sont touchés par chacune des vulnérabilités, et quelles menaces sont ainsi plus susceptibles de se concrétiser.

6.2.2 Biens touchés

Certaines vulnérabilités ont de vastes répercussions touchant de nombreux biens et valeurs des biens, alors que d'autres ont une incidence plus restreinte. Par exemple, des politiques et procédures déficientes en matière de sécurité peuvent exposer pratiquement tous les biens et toutes les valeurs des biens à une compromission, alors que l'utilisation d'une déchiqueteuse non approuvée pour détruire les documents classifiés n'a de répercussion que sur le risque de divulgation non autorisée de renseignements confidentiels, ce qui constitue une vulnérabilité liée à la confidentialité, plutôt qu'à un problème de disponibilité ou d'intégrité. L'établissement de liens explicites entre les vulnérabilités et les biens à risque, généralement aux niveaux des groupes ou des sous-groupes, constitue un aspect important de l'évaluation des vulnérabilités, et sert trois fins d'analyse :

- premièrement, à restreindre la portée du projet d'EMR et mettre l'accent sur les risques les plus importants, c'est-à-dire sur les vulnérabilités les plus graves touchant des biens de plus grande valeur;
- deuxièmement, à déterminer si une évaluation étendue des vulnérabilités est nécessaire en vertu de la section 6.1.3 ci-dessus, à cause de faiblesses connexes touchant le même bien;
- troisièmement, à organiser les données relatives aux trois variables de risque (valeurs des biens, menaces et vulnérabilités) en prévision du calcul du risque résiduel.

6.2.3 Menaces favorisées

De la même manière, certaines vulnérabilités favorisent la réalisation de beaucoup de menaces distinctes, alors que d'autres ne sont associées qu'à quelques menaces. Sur le plan de la sécurité matérielle, par exemple, des contrôles d'accès inadéquats accroissent la probabilité de compromission attribuable à pratiquement toutes les menaces délibérées et à bon nombre d'accidents, ce qui a des conséquences défavorables sur la confidentialité, la disponibilité et l'intégrité. Par contre, il est peu probable que des mesures de sécurité inadéquates des émissions soient exploitées autrement que par un service de renseignement hautement spécialisé. L'établissement de liens potentiels entre les vulnérabilités et les menaces connexes offre des avantages comparables pour la concentration sur les risques les plus importants, principalement ceux qui découlent des menaces les plus graves exploitant les vulnérabilités les plus importantes et exposant les biens ayant la plus grande valeur.

6.2.4 Renvois pratiques

Certains documents offrent une orientation permettant de garantir une approche structurée et méthodique pour l'identification des vulnérabilités et des biens et menaces connexes :

- **Appendice D-2**, **Liste des vulnérabilités**, où sont définies les valeurs des biens exposés à un risque de compromission pour chaque vulnérabilité;
- **Section 4.2 de l'annexe B, Phase d'identification et d'évaluation des biens**, où sont examinées les valeurs des biens associées aux différentes classes de bien;
- **Section 2.6 de l'annexe C**, **Phase d'évaluation des risques**, où sont fournis des renseignements sur les catégories et les valeurs des biens touchés par chacune des menaces, ainsi que les types de compromission.

6.3 Résumé

La détermination des niveaux des vulnérabilités en fonction de leur incidence sur la probabilité de compromission (faiblesses relatives aux mesures de prévention) et la gravité des conséquences (faiblesses relatives aux mécanismes de détection, de réaction et de reprise) constitue l'un des fondements de la méthodologie harmonisée d'EMR pour définir des paramètres communs et permettre les analyses comparatives. On trouve à l'appendice D-3 des directives et des explications détaillées concernant les cinq processus de l'évaluation des vulnérabilités.

7 Tableau priorisé d'évaluation des vulnérabilités

Comme il en est question ci-dessus, une cote relative doit être attribuée à toutes les vulnérabilités présentant des risques pour les biens inclus dans une évaluation des menaces et identifiées à la troisième phase du projet d'EMR, en fonction de leur incidence sur la probabilité de compromission et la gravité des conséquences. Une seule vulnérabilité peut mettre en péril un ou plusieurs biens et favoriser la réalisation d'une ou de plusieurs menaces. Cette information doit être consignée dans le tableau d'évaluation des vulnérabilités, résultat final de l'évaluation des vulnérabilités réalisée dans le cadre de la phase d'évaluation des risques d'un projet d'EMR. Il suffit de trier ensuite les cotes des vulnérabilités en ordre croissant (de Très faible à Très élevée) pour établir rapidement l'ordre de priorité de chacune des vulnérabilités et cerner les plus importantes.

Ce tableau ressemble à celui qui suit (tableau D-5); l'appendice D-4 présente plus de détails.

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Vulnérabilités connexes	Niveau	Bien(s) exposé(s)	Menace(s) favorisée(s)

Tableau D-5 : Exemple de tableau d'évaluation des vulnérabilités

Page intentionnellement laissée en blanc

Appendice D-1 - Sources de données sur les vulnérabilités

Ressources ministérielles	
Source de données/Documentation	**Classe/groupe de vulnérabilités**
Gestionnaires de programme • Plans d'activités • Procédures normales d'exploitation	• Programme de sécurité o Rôles et responsabilités o Ressources humaines o Ressources financières o Procédures de sécurité • Partage de l'information et des biens o Information • Marchés • Identification des biens • Sanctions
Gestionnaires du matériel/des biens • Répertoires des biens • Procédures normales d'exploitation	• Marchés • Sécurité matérielle o Entreposage sécurisé
Gestionnaires des installations • Plans d'étage/schémas des immeubles • Rapports des gardes • Procédures de contrôle d'accès • Plans d'intervention d'urgence • Rapports d'incidents	• Partage de l'information et des biens o Installations • Protection des employés o Réponse de la direction/Mesures de protection • Sécurité matérielle o Sécurité du périmètre o Contrôles d'accès o Gestion des installations
Ressources humaines • Rapports d'incidents	• Protection des employés
Finances • Procédures normales d'exploitation	• Restrictions d'accès o Disponibilité/intégrité/séparation des tâches
Dirigeant principal de l'information • Accords sur les niveaux de service • Modalités de partage des biens • Normes/Directives en matière de sécurité des TI	• Partage de l'information et des biens o Infrastructure des TI • Sécurité des TI o Contrôles de gestion o (Quelques) mesures de protection techniques o Mesures de protection opérationnelles

Ressources ministérielles	
Source de données/Documentation	**Classe/groupe de vulnérabilités**
Administrateur (de la sécurité) des systèmes • Schémas des systèmes • Procédures normales d'exploitation • Tests de sécurité/rapports d'évaluation • Registres/rapports des incidents	• Sécurité des TI o (Quelques) contrôles de gestion o Mesures de protection techniques o Mesures de protection opérationnelles
Agent de sécurité du ministère • Directives ministérielles sur la sécurité • Procédures normales d'exploitation • Rapports d'inspection sur la sécurité • Rapports d'enquête	• Programme de sécurité • Marchés • Sensibilisation/formation en matière de sécurité • Identification des biens • Gestion des risques liés à la sécurité • Filtrage de sécurité • Protection des employés • Sécurité matérielle • Sécurité en situations d'urgence • Enquête sur les incidents • Sanctions
Coordonnateur de la sécurité des TI • Examens/évaluations des produits • Rapports d'incidents	• Enquêtes/incidents concernant la sécurité des TI
Coordonnateur de la PCA • Plans de continuité des activités • Exercice sur les PCA/résultats des tests	• Planification de la continuité des activités
Vérification interne/examen • Vérifications/examens de la sécurité	• Programme de sécurité (tout contrôle de gestion assujetti à une vérification ou à un examen)
Santé et sécurité au travail • Procédures normales d'exploitation • Rapports d'enquête/d'incident	• Protection des employés o Gestion des incidents

Ressources externes : Ministères responsables de la sécurité	
Source de données/Documentation	**Type de vulnérabilités**
Centre de la sécurité des télécommunications http://www.cse-cst.gc.ca/publications/publications-f.html • Conseils en matière de sécurité des TI • Alertes de sécurité des TI • Bulletins de sécurité TI http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-f.html • Rapports de certification de produits évalués	• Sécurité des TI
Sécurité publique et Protection civile Canada • http://www.ps-sp.gc.ca/prg/em/ccirc/anre-fr.asp • Diffusions/avis analytiques	• Sécurité des TI
Gendarmerie royale du Canada • http://www.rcmp.ca/tsb/home_f.htm • Guides/rapports en sécurité	• Sécurité matérielle • Sécurité des TI

Ressources externes : Secteur privé	
Source de données	**Type de vulnérabilités**
Bases de données des avis de vulnérabilité de US-CERT (États-Unis) http://www.kb.cert.org/vuls	• Vulnérabilités techniques
Critères communs (en anglais) http://www.commoncriteriaportal.org/public/consumer	• Produits de sécurité des TI évalués • Vulnérabilités connexes
Archives des analyses de vulnérabilités critiques de l'Institut SANS (en anglais) http://www.sans.org/newsletters/cva/index.php	• Vulnérabilités techniques
Fournisseurs de produits	• Vulnérabilités techniques

Nota :

1. Cette liste n'est pas exhaustive. D'autres éléments s'y ajouteront occasionnellement. Toute suggestion de documents de référence ou de contacts à ajouter peut être présentée aux bureaux mentionnés dans l'avant-propos.
2. L'inclusion d'un site Web ne doit pas être interprétée comme une approbation. De la même manière, l'exclusion de sources qui pourraient se révéler utiles ne signifie pas qu'elles sont rejetées. La liste vise simplement à illustrer la richesse des renseignements facilement accessibles aux spécialistes de la sécurité et aux gestionnaires de risques.

Page intentionnellement laissée en blanc

Appendice D-2 - Liste des vulnérabilités

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Incidence			Valeurs en cause		
			O_{Prob}	C_{Prob}	C_{Grav}	C	D	I
Programme de sécurité	Rôles et responsabilités	Haute direction		√	√	√	√	√
		Gestionnaires de programme		√	√	√	√	√
		Gestionnaires de projet		√	√	√	√	√
		Dirigeant principal de l'information		√	√	√	√	√
		Employés		√	√	√	√	√
		ASM		√	√	√	√	√
		Coordonnateur de la sécurité des TI		√	√	√	√	√
		Gardien COMSEC		√	√	√	√	√
		Coordonnateur de la PCA		√	√		√	
	Ressources humaines	Effectif		√	√	√	√	√
		Niveaux de classification		√	√	√	√	√
	Ressources financières	Activités ministérielles		√	√	√	√	√
		Projets		√	√	√	√	√
	Politique/procédures de sécurité	Partage d'information/de biens		√	√	√	√	√
		Marchés		√	√	√	√	√
		Formation/sensibilisation en matière de sécurité		√	√	√	√	√
		Identification des biens		√	√	√	√	√
		Gestion des risques liés à la sécurité		√	√	√	√	√
		Restrictions d'accès		√	√	√	√	√
		Filtrage de sécurité		√	√	√	√	√
		Protection des employés		√	√	√	√	√
		Sécurité matérielle		√	√	√	√	√
		Sécurité des TI		√	√	√	√	√
		Sécurité en situations d'urgence		√	√	√	√	√
		Planification de la continuité des activités		√	√	√	√	√
		Vérification du programme de sécurité		√	√	√	√	√
		Enquête sur les incidents		√	√	√	√	√
		Sanctions		√	√	√	√	√
Partage d'information/de biens	Information	Modalités		√	√	√	√	√
	Installations	Modalités		√	√	√	√	√
	Infrastructure des TI	Modalités		√	√	√	√	√
Sécurité à l'extérieur du Canada	Normes spéciales	Une EMR par emplacement		√	√	√	√	√
	Restrictions sur les voyages	Selon l'établissement	√	√	√	√	√	√
Marchés	Rôles et responsabilités	Autorité technique/chargé de projet		√		√		

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Incidence			Valeurs en cause		
			O_{Prob}	C_{Prob}	C_{Grav}	C	D	I
	LVERS			√		√		
	Attestation de sécurité des installations	Personnel responsable		√		√		
		Protection des documents		√		√		
	Marchés internationaux			√		√		
Formation/sensibilisation en matière de sécurité	Rôles et responsabilités	Agent de formation et de sensibilisation	√	√	√	√	√	√
	Formation en matière de sécurité	Spécialistes de la sécurité	√	√	√	√	√	√
	Sensibilisation à la sécurité	Séances d'information initiales	√	√	√	√	√	√
		Mises à jour régulières	√	√	√	√	√	√
Identification des biens	Confidentialité	Catégorisation : Classifié		√	√	√		
		Marquage : Classifié		√	√	√		
		Catégorisation : Protégé		√	√	√		
		Marquage : Protégé		√	√	√		
	Disponibilité	Catégorisation		√	√		√	
		Marquage		√	√		√	
	Intégrité	Catégorisation		√	√			√
		Marquage		√	√			√
Gestion des risques liés à la sécurité	EMR	Filtrage initial	√	√	√	√	√	√
		Surveillance continue	√	√	√	√	√	√
Restrictions d'accès	Biens classifiés/protégés	Besoin de connaître		√	√	√		
		Filtrage de sécurité		√	√	√	√	√
	Disponibilité/Intégrité	Division des tâches	√	√	√	√	√	√
Filtrage de sécurité	Cote de fiabilité	Établissement des exigences		√		√	√	√
		Filtrage initial		√		√	√	√
		Évaluation des résultats		√		√	√	√
		Mises à jour régulières		√		√	√	√
		Examen justifié			√	√	√	√
		Révocation			√	√	√	√
		Procédures de diffusion			√	√	√	√
	Habilitation de sécurité	Établissement des exigences		√		√		
		Filtrage initial		√		√		
		Évaluation des résultats		√		√		
		Mises à jour régulières		√		√		
		Examen justifié			√	√		
		Révocation/déclassement			√	√		
		Procédures de diffusion			√	√		
	Autorisation d'accès au site	Établissement des exigences		√		√		
		Filtrage initial		√		√		
		Évaluation des résultats		√		√		
		Mises à jour régulières		√		√		
		Examen justifié			√	√		
		Révocation			√	√		
		Procédures de diffusion			√	√		
Protection des employés	Identification des employés à risque	EMR		√	√	√		

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Incidence			Valeurs en cause		
			O_{Prob}	C_{Prob}	C_{Grav}	C	D	I
	Réponse de la direction	Mesures de protection		√	√	√		
		Mécanismes de soutien		√	√	√		
		Formation et counselling		√	√	√		
	Gestion des incidents	Rapports d'incident			√	√		
		Enquête sur les incidents			√	√		
		Mesures correctives			√	√		
Sécurité matérielle	Facteurs de planification	Codes du bâtiment		√	√	√	√	√
		Zones de sécurité		√	√	√	√	√
	Sélection de sites	Servitudes	√				√	
		Voies d'urgence	√				√	
		Emplacement/topographie de l'immeuble	√				√	
		Services d'urgence	√				√	
		Occupants adjacents	√			√	√	
	Sécurité du périmètre	Contrôle du périmètre du site		√	√	√	√	√
		Éclairage du site	√		√	√	√	√
		Signalisation extérieure	√			√	√	√
		Aménagement paysager		√	√	√	√	√
		Stationnement		√	√	√	√	√
	Sécurité à l'entrée	Entrées pour piétons/halls d'entrée		√		√	√	√
		Accès aux services publics		√		√	√	√
		Aires de réception/d'expédition		√		√	√	√
	Planification de la sécurité à l'intérieur	Voies de circulation		√	√		√	
		Halls des ascenseurs		√	√		√	
		Garderies		√	√		√	
		Salles de réunion/conférence		√	√	√	√	
		Escaliers/ascenseurs		√	√		√	
		Toilettes		√	√		√	
		Aires d'agrément		√	√		√	
		Salles du courrier		√	√	√	√	
		Télécommunications/câblage		√	√	√	√	√
		Aires de CVC		√	√		√	
		Salles des serveurs		√	√	√	√	√
	Contrôles d'accès	Cartes d'identité		√		√	√	√
		Contrôles d'accès électroniques		√		√	√	√
		Dispositifs électroniques de détection des intrusions			√	√	√	√
		Équipement vidéo en circuit fermé			√	√	√	√
		Centre de contrôle de la sécurité		√	√	√	√	√
		Locaux de réunion sécurisés		√		√		
		Chambres fortes		√		√	√	√
		Gardes de sécurité		√	√	√	√	√
	Gestion des installations	Contrats de location		√		√	√	√
		Services d'entretien		√		√	√	√
		Services de nettoyage		√		√	√	√

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Incidence			Valeurs en cause		
			O_{Prob}	C_{Prob}	C_{Grav}	C	D	I
		Signalisation intérieure	√			√	√	√
		Dispositif de verrouillage/ contrôle des clés		√		√	√	√
		Travaux de rénovation		√		√	√	√
		Comité de sécurité des installations		√		√	√	√
	Entreposage sécurisé	Contenants de sécurité		√		√	√	√
		Clés/combinaisons		√		√	√	√
		Entretien des conteneurs		√		√	√	√
		Élimination des contenants		√		√	√	√
		Salles sécurisées/chambres fortes		√		√	√	√
	Transport/Transmission	Transport		√		√	√	√
		Transmission		√		√	√	√
	Destruction	Entreposage en attendant l'élimination		√		√		
		Équipement de destruction : papier		√		√		
		Équipement de destruction : soutien des TI		√		√		
		Marquage de l'équipement		√		√		
		Entretien de l'équipement		√		√		
		Services contractuels		√		√		
		Destruction d'urgence		√		√		
Sécurité des TI	Contrôles de gestion	Cycle de développement de système		√	√	√	√	√
		Ressources destinées aux projets de sécurité des TI		√	√	√	√	√
		Certification et accréditation		√	√	√	√	√
		Marchés		√	√	√	√	√
		Impartition		√	√	√	√	√
	Mesures de protection techniques	Produits évalués		√	√	√	√	√
		Identification et authentification		√		√	√	√
		Autorisation et contrôle de l'accès		√		√	√	√
		Chiffrement		√		√		√
		Infrastructure à clé publique (ICP)		√		√	√	√
		Défense du périmètre		√		√	√	√
		Informatique mobile/télétravail		√		√	√	√
		Dispositifs sans fil		√		√	√	√
		Sécurité des émissions		√		√		
		Câbles de télécommunication		√		√	√	
		Intégrité des logiciels		√		√	√	√
		Configuration des logiciels de sécurité		√		√	√	√
		Protection contre les codes malveillants		√	√		√	√

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Incidence			Valeurs en cause		
			O_{Prob}	C_{Prob}	C_{Grav}	C	D	I
		Détection des intrusions			√	√	√	√
		Protection/reprise			√		√	
	Mesures de protection opérationnelles	Service de dépannage/résolution des problèmes		√	√	√	√	√
		Gestion des incidents		√	√	√	√	√
		Évaluations des vulnérabilités		√		√	√	√
		Gestion des correctifs		√		√	√	√
		Planification de la continuité des activités des TI			√	√	√	√
		Évaluation et vérification de la sécurité des TI		√	√	√	√	√
		Gestion des configurations		√		√	√	√
		Contrôle des changements		√		√	√	√
		Planification de la capacité		√			√	
		Entretien du matériel		√	√	√	√	√
		Protection de l'environnement			√		√	
		Conditionnement d'alimentation/ alimentation de secours			√		√	
Sécurité en situations d'urgence	Plans et procédures	Plans ministériels		√	√		√	
		Essais		√	√		√	
		Coordination avec d'autres plans		√	√		√	
		Attribution de ressources durables		√	√		√	
Planification de la continuité des activités	Structure de gouvernance	Pouvoirs			√		√	
		Responsabilités			√		√	
	Analyse des répercussions sur les activités				√		√	
	Plans/Modalités				√		√	
	Préparation du programme de PCA				√		√	
	Examens, essais et vérification				√		√	
Enquête sur les incidents	Enquête sur les incidents			√	√	√	√	√
	Rapports d'incident			√	√	√	√	√
Sanctions	Atteintes à la sécurité		√			√	√	√
	Infractions à la sécurité		√			√	√	√

Nota :

1. Le ou les principaux effets des vulnérabilités attribuables aux insuffisances de n'importe quelle mesure de protection sont indiqués dans ce tableau dans la colonne de l'incidence :
   - **O_{Prob}** – augmentation de la probabilité d'occurrence d'une menace, habituellement à cause de la faiblesse des mécanismes de dissuasion ou d'évitement;
   - **C_{Prob}** – augmentation de la probabilité d'une compromission si une menace s'est matérialisée, habituellement à cause de mesures de prévention inadéquates;

- o **C_{Grav}** – augmentation de la gravité des conséquences d'un incident, à cause de mesures de détection, d'intervention ou de reprise inefficaces.

2. Les valeurs qui seront les plus vraisemblablement en cause sont indiquées dans les trois dernières colonnes, c'est-à-dire confidentialité (C), disponibilité (D) et intégrité (I) du bien.
3. Cette liste n'est pas un relevé exhaustif des incidences ou des valeurs des biens. Elle donne plutôt des indications générales pour faciliter l'analyse pendant l'évaluation des vulnérabilités.

Appendice D-3 - Paramètres des vulnérabilités

1 Instructions

Dans le cadre du projet d'EMR, il faut déterminer le niveau approprié de chaque vulnérabilité évaluée qui expose des biens à une menace, en procédant ainsi :

- **Étape 1.** Déterminez toutes les mesures de protection existantes et, dans le contexte du projet, les mesures de protection proposées pour les biens visés par l'évaluation, à partir de la liste des mesures de protection de l'appendice F-2.
- **Étape 2.** Déterminez les fonctions de sécurité (évitement, dissuasion, prévention, détection, intervention et reprise) de chaque mesure de protection.
- **Étape 3.** Déterminez les vulnérabilités possibles pour chaque mesure de protection qui a été, sera ou aurait dû être mise en œuvre conformément aux normes de sécurité de référence, en vous inspirant de la liste des vulnérabilités de l'appendice D-2.
- **Étape 4a.** Évaluez l'incidence de chaque vulnérabilité sur la probabilité de compromission sur une échelle allant de Faible à Élevée ou indiquez « sans objet » en l'absence de fonction de prévention, conformément au tableau D3-1 ci-dessous.

Efficacité des mesures de protection	Vulnérabilités connexes	Probabilité de compromission
Aucune mesure de protection Mesure inefficace en grande partie Probabilité de compromission > 75 %	Facilement exploitables Besoin de peu de connaissances/ compétences/ressources Biens hautement accessibles Biens très complexes/fragiles/portables Employés mal informés/formés	Élevée
Mesure modérément efficace Probabilité de compromission 25-75 %	Pas facilement exploitables Besoin de certaines connaissances/ compétences/ressources Biens modérément accessibles Biens modérément complexes/fragiles/portables Employés modérément informés/formés	Moyenne
Mesure très efficace Probabilité de compromission < 25 % (Mesure remplissant uniquement des fonctions de détection, de réaction ou de reprise)	Difficiles à exploiter Besoin de très bonnes connaissances/ compétences/ressources Accès aux biens rigoureusement contrôlé Biens très simples/robustes/statiques Employés bien informés/formés	Faible (sans objet)

Tableau D3-1 : Incidence des vulnérabilités sur la probabilité de compromission (prévention)

- **Étape 4b.** Évaluez l'incidence de chaque vulnérabilité sur la gravité des conséquences sur une échelle allant de Faible à Élevée ou indiquez « sans objet » en l'absence de fonction de détection, de réaction ou de reprise, conformément au tableau D3-2 ci-dessous.

Efficacité des mesures de protection	Vulnérabilités connexes	Gravité des conséquences
Aucune mesure de protection Mesure en grande partie inefficace Biens exposés à des préjudices importants	Détection improbable des compromissions Dommage difficile à contenir Délais de reprise prolongés/Niveaux de service faibles Biens très complexes/fragiles Employés mal informés/formés	Élevée
Mesure modérément efficace Biens exposés à des préjudices modérés	Compromissions probablement détectées au fil du temps Dommages partiellement contenus Délais de reprise/Niveaux de services modérés Biens relativement complexes/fragiles Employés modérément informés/formés	Moyenne
Mesure très efficace Biens exposés à des préjudices limités (Mesures de protection ayant pour seule fonction la prévention)	Compromissions presque certainement détectées rapidement Dommages rigoureusement contenus Reprise rapide et complète Biens très simples/robustes Employés bien informés/formés	Faible (Sans objet)

Tableau D3-2 : Incidence des vulnérabilités sur la gravité des conséquences (détection, réaction ou reprise)

- **Étape 5a.** Déterminez le niveau de chaque vulnérabilité sur une échelle allant de Très faible à Très élevé en mettant en corrélation son incidence sur la probabilité de compromission (axe horizontal du tableau D3-3, Évaluation de base des vulnérabilités) et l'incidence sur la gravité des conséquences (axe vertical).

Incidence sur la gravité des conséquences (détection, réaction et reprise)	Incidence sur la probabilité de compromission (prévention)		
	Faible (S.O.)	**Moyenne**	**Élevée**
Élevée	Moyenne	Élevée	Très élevée
Moyenne	Faible	Moyenne	Élevée
Faible (s.o.)	Très faible	Faible	Moyenne

Tableau D3-3 : Évaluation de base des vulnérabilités

- **Étape 5b.** Pour les vulnérabilités cotées Faible, Moyenne ou Élevée à l'étape 5a, procédez à une évaluation étendue des vulnérabilités:
    - s'il s'agit d'une vulnérabilité cotée Faible, Moyenne ou Sans objet du point de vue de l'incidence sur la probabilité de compromission, déterminez si toute vulnérabilité connexe est cotée Moyenne ou Élevée à cause de la faiblesse des mesures de prévention;
    - si une vulnérabilité connexe a une incidence plus élevée sur la probabilité de compromission, recalculez la vulnérabilité globale au tableau D3-3 au moyen de ces valeurs plus élevées;
    - s'il s'agit d'une vulnérabilité cotée Faible, Moyenne ou Sans objet du point de vue de l'incidence sur la gravité des conséquences, déterminez si toute vulnérabilité connexe est cotée Moyenne ou Élevée à cause de la faiblesse des mesures de prévention, d'intervention ou de reprise;
    - si une vulnérabilité connexe a une incidence plus élevée sur la gravité des conséquences, recalculez la vulnérabilité globale au tableau D3-3 au moyen de ces valeurs plus élevées.
- **Étape 5c.** Déterminez quels biens identifiés lors de la phase d'identification et d'évaluation des biens (annexe B) sont exposés et quelles menaces identifiées lors de la phase d'évaluation des menaces (annexe C) sont favorisées par chaque vulnérabilité, ou paire de vulnérabilités connexes dans le cas d'une évaluation étendue des vulnérabilités.
- **Étape 5d.** Si vous avez encore un doute au sujet du niveau réel de vulnérabilité, vous pouvez entrer la valeur la plus faible et la valeur la plus élevée dans le tableau d'évaluation des vulnérabilités et vous en servir pour calculer le risque résiduel pendant la phase d'évaluation des risques, afin d'établir si cette incertitude se répercute sur le risque résiduel évalué.
- **Étape 5e.** Si une vulnérabilité se rapproche de la ligne de démarcation entre deux niveaux, il convient de la baliser au moyen de flèches (↑↓) indiquant si elle se rapproche de l'extrémité supérieure ou de l'extrémité inférieure de la fourchette; elle pourra ainsi faire l'objet d'une analyse subséquente lors de la phase d'évaluation des risques. Par exemple, si une compromission est susceptible d'être décelée dans les 24 à 48 heures, la gravité des résultats pourra être faible, mais se rapprocher de la gravité moyenne, de sorte que le niveau final de la vulnérabilité devrait être marqué d'une flèche ascendante (↑).
- **Étape 6.** Entrez les résultats dans les colonnes appropriées du tableau d'évaluation des vulnérabilités de l'appendice D-4.

2 Exemples

2.1 Éclairage de périmètre insuffisant

Le processus analytique exposé ci-dessus pourrait être appliqué de la façon suivante pour déterminer les niveaux de vulnérabilité associés à un éclairage de périmètre insuffisant :

- **Identification de la mesure de protection.** La section 7.3.6 de la *Norme opérationnelle sur la sécurité matérielle* stipule notamment que l'« éclairage devrait être suffisant dans les installations et autour de celles-ci afin de permettre la détection et

l'observation des personnes qui approchent des installations », ce que confirme le *Guide G1-002 de la GRC, Éclairage de sécurité*.

- **Fonctions de sécurité.** Comme le précise la norme opérationnelle de sécurité, un éclairage adéquat peut décourager certains types d'attaques délibérées, comme le vol ou le vandalisme, et donc réduire la probabilité qu'une menace se concrétise. Cet effet de dissuasion pourrait être pris en considération dans la phase d'évaluation des menaces d'un projet d'EMR, conformément à la section 5.1 de l'annexe D. Toutefois, aux fins de l'évaluation des vulnérabilités, il faut déterminer si l'éclairage de périmètre remplit des fonctions de prévention, de détection, de réaction ou de reprise. À cet égard, des lumières à elles seules n'arrêteront rien, de sorte qu'elles ne représentent pas une mesure de prévention en soi. Par ailleurs, il est beaucoup plus facile d'apercevoir un intrus dans un lieu bien éclairé. C'est pourquoi l'éclairage de périmètre est un important mécanisme de détection lorsqu'il s'agit d'amorcer une intervention qui pourrait contribuer à restreindre le préjudice ou à réduire la gravité des conséquences advenant un compromission.
- **Vulnérabilités connexes.** Un éclairage de sécurité inadéquat, qui constitue la vulnérabilité en cause, aurait l'effet contraire, c'est-à-dire qu'il accroîtrait le préjudice susceptible de se produire si les agents de menace poursuivent leurs activités illicites sans être interrompus.
- **Incidence de la vulnérabilité sur la probabilité de compromission (prévention).** Comme l'éclairage de périmètre ne constitue pas une mesure de prévention, les faiblesses qui lui sont associées n'auront pas de répercussions sur la probabilité de compromission. Il convient donc d'attribuer à cette vulnérabilité la cote faible, ou plus précisément, la cote Sans objet au tableau D3-1, Incidence des vulnérabilités sur la probabilité de compromission (prévention).
- **Incidence de la vulnérabilité sur la gravité des conséquences (détection, réaction et reprise).** S'il n'y a pas de lumières du tout ou si elles sont faibles et sales, l'incidence sur la gravité des conséquences pourrait être élevée, conformément au tableau D3-2, Incidence des vulnérabilités sur la gravité des conséquences (détection, réaction ou reprise). Des lumières de basse intensité qui assurent un certain éclairage et qui offrent donc des chances modérées de détecter quiconque s'attarde dans le secteur pourraient se voir attribuer la cote Moyenne, tandis que des lampes à vapeur de mercure de haute intensité placées à intervalles réguliers sur tout le périmètre pourraient accroître sensiblement la probabilité de détection et ainsi réduire à faible l'incidence sur la gravité des conséquences.
- **Évaluation de base de la vulnérabilité.** Si l'incidence sur la probabilité de compromission est faible ou sans objet, la cote de l'évaluation de base de la vulnérabilité serait choisie dans la première colonne du tableau D3-3 et elle serait Très faible, Faible ou Moyenne, selon l'incidence sur la gravité des conséquences déterminée à l'étape précédente.
- **Évaluation étendue de la vulnérabilité.** L'incidence sur la probabilité de compromission a été cotée Sans objet; il faut donc faire une évaluation étendue de la vulnérabilité pour déterminer s'il y a des vulnérabilités connexes attribuables à des mesures de prévention inadéquates, par exemple des contrôles d'accès qui sont insuffisants, des fenêtres en verre qui ne sont pas protégées ou des serrures non approuvées sur les portes extérieures. Si l'une ou l'autre de ces faiblesses est cotée Moyenne ou Élevée du point de vue de son incidence sur la probabilité de

compromission, la cote de l'évaluation étendue de la vulnérabilité pourrait être Élevée ou Très élevée.

- **Biens exposés/Menaces favorisées.** Selon la portée du projet d'EMR, un éclairage de périmètre inadéquat pourrait exposer divers biens à un risque accru. Parmi les exemples les plus flagrants, citons tout employé qui fréquente les lieux et le contenu de l'installation. Les menaces qu'un éclairage insuffisant pourrait favoriser vont des graffitis laissés sur les murs extérieurs par des vandales jusqu'aux prédateurs qui traquent des piétons, en passant par les cambrioleurs qui ciblent l'équipement ou les fournitures.

2.2 Mesures de protection désuètes contre les codes malveillants

Les niveaux de vulnérabilité associés à des logiciels antivirus désuets peuvent être déterminés selon la même procédure.

- **Identification de la mesure de protection.** La section 6.4.12 de la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)* stipule notamment que les « ministères doivent régulièrement installer, utiliser et mettre à jour des logiciels antivirus et effectuer un balayage pour repérer les codes malveillants sur tous les fichiers électroniques provenant de l'extérieur. »
- **Fonctions de sécurité.** Même si les fonctions et les caractéristiques des logiciels antivirus varient considérablement, la plupart assure deux fonctions de sécurité, voire plus : la détection précoce d'un code malveillant avant qu'il ne soit exécuté est en fait une mesure de prévention, alors que la reconnaissance d'activités ou de comportements suspects est un mécanisme de détection qui peut déclencher une intervention en vue d'éteindre l'appareil infecté ou d'empêcher la propagation du virus.
- **Vulnérabilités connexes.** Les logiciels antivirus doivent être mis à jour régulièrement, pour être en mesure de reconnaître les dernières menaces et d'y réagir, et des vulnérabilités pouvant se révéler graves risquent d'accroître la probabilité de compromission autant que la gravité des conséquences.
- **Incidence de la vulnérabilité sur la probabilité de compromission (prévention).** Si les logiciels sont mis à jour automatiquement en temps réel, ils représentent une mesure de protection très efficaces et l'incidence sur la probabilité de compromission serait faible. S'il se passe plusieurs jours ou plusieurs semaines entre les mises à niveau, la probabilité qu'un virus soit détecté diminue sensiblement, de sorte que l'incidence serait moyenne. Si les logiciels ne sont jamais mis à jour ou s'ils n'ont pas été installés correctement dès le départ, les répercussions sur la probabilité de compromission seraient élevées.
- **Incidence de la vulnérabilité sur la gravité des conséquences (détection, réaction et reprise).** Des logiciels antivirus désuets sont également moins susceptibles de détecter des virus et des vers nouveaux et d'y réagir, de sorte que leur incidence sur la gravité des conséquences s'accroîtra au fil de temps, passant de faible pour la version courante à élevée pour des versions véritablement désuètes.
- **Évaluation de base de la vulnérabilité.** Selon les cotes attribuées aux deux dimensions de la vulnérabilité (probabilité de compromission et gravité des conséquences), la cote de l'évaluation de base pourrait aller de Très faible (pour les

logiciels les plus récents qui sont très efficaces) à Très élevée (pour les versions totalement désuètes).

- **Évaluation étendue de la vulnérabilité.** En pareil cas, il conviendrait de faire une évaluation étendue seulement si des insuffisances dans les mesures de protection contre des codes malveillants se sont vu attribuer la cote Faible ou Moyenne au chapitre de la prévention (probabilité de compromission) ou de la détection et de l'intervention (gravité des conséquences).
- **Biens exposés/Menaces favorisées.** Dans le cas qui nous occupe, les vulnérabilités attribuables à l'insuffisance des mesures de protection contre des codes malveillants pourraient exposer un petit groupe de biens à des risques accrus; il s'agit expressément des fichiers électroniques dans les systèmes et des services qui s'en servent. De toute évidence, la principale menace découlant de cette vulnérabilité est le sabotage de la part de pirates informatiques, qu'il s'agisse de particuliers, de groupes ou d'organisations parrainées par un État.

Appendice D-4 - Tableau d'évaluation des vulnérabilités

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Vulnérabilités connexes	Niveau	Bien(s) exposé(s)	Menace(s) favorisée(s)
Programme de sécurité						
Partage d'information/de biens						
Sécurité à l'extérieur du Canada						
Marchés						
Sensibilisation/formation en matière de sécurité						
Identification des biens						
Gestion des risques liés à la sécurité						
Restrictions d'accès						
Filtrage de sécurité						
Protection des employés						
Sécurité matérielle						
Sécurité des TI						
Sécurité en situations d'urgence						
Planification de la continuité des activités						
Enquête sur les incidents						
Sanctions						

1 Instructions

Entrez toutes les vulnérabilités qui exposent les biens visés par le projet d'EMR aux menaces déterminées pendant la phase d'évaluation des menaces, en vous inspirant de la liste des vulnérabilités de l'appendice D-2.

À partir des paramètres des vulnérabilités de l'appendice D-3, déterminez le niveau pertinent de chaque vulnérabilité sur une échelle allant de Très faible (TF) à Très élevé (TE), en fonction de l'évaluation de base ou de l'évaluation étendue des vulnérabilités, le cas échéant.
Indiquez les biens exposés par ces vulnérabilités et les menaces qu'elles favorisent.

2 Exemples

Pour les deux exemples présentés dans l'appendice D-3 (éclairage de périmètre insuffisant et mesures de protection désuètes contre les codes malveillants), le tableau serait rempli ainsi :

Classe de vulnérabilité	Groupe de vulnérabilités	Vulnérabilité	Vulnérabilités connexes	Niveau	Bien(s) exposé(s)	Menace(s) favorisée(s)
Sécurité matérielle	Sécurité du périmètre	Éclairage de périmètre insuffisant	Contrôles d'accès faibles	E[1]	Employés Extérieur de l'immeuble	Prédateurs Vandales
			Fenêtres non protégées	TE[2]	Contenu de l'immeuble	Cambrioleurs
Sécurité des TI	Mesures de protection techniques	Logiciels antivirus désuets	S.O.	M[3]	Fichiers élec. Services connexes	Pirates informatiques

[1] En supposant que l'éclairage de périmètre est particulièrement mauvais ou inexistant comme mécanisme de détection et qu'il mérite une cote élevée du point de vue de l'incidence sur la gravité des conséquences, alors que les contrôles d'accès au périmètre sont jugés moyennement efficaces et méritent une cote moyenne du point de vue de l'incidence sur la probabilité de compromission.

[2] En supposant ici aussi que l'éclairage de périmètre est particulièrement mauvais ou inexistant comme mécanisme de détection et qu'il mérite une cote élevée du point de vue de l'incidence sur la gravité des conséquences, alors que les fenêtres en verre de l'immeuble ne sont pas protégées et qu'elles méritent donc une cote élevée du point de vue de l'incidence sur la probabilité de compromission.

[3] En supposant que les logiciels antivirus sont mis à jour à des intervalles de quelques semaines plutôt que tous les jours, ou encore mieux en temps réel, de sorte que leur incidence sur la probabilité de compromission et sur la gravité des conséquences mériterait une cote moyenne qui donnerait lieu à une cote globale moyenne à l'évaluation de base de la vulnérabilité.

Annexe E - Calcul des risques résiduels

1 Introduction

1.1 Généralités

Le deuxième volet de la phase d'évaluation des risques d'un projet d'EMR est le calcul des risques résiduels, qui comprend un seul processus et un résultat important, soit :

- **Calcul des risques résiduels** – établir des cotes des risques résiduels (allant de Très faible à Très élevé) en fonction des valeurs des biens identifiés dans la portée de l'évaluation, des menaces connexes susceptibles de compromettre ces biens, les employés et les services, ainsi que de toute vulnérabilité associée.
- **Liste des risques résiduels classés par ordre de priorité** – Production d'une liste exhaustive des risques résiduels, classés en ordre décroissant de gravité.

1.2 But

Le but de cette annexe est de décrire le processus et le résultat unique du volet de calcul des risques résiduels de la phase d'évaluation des risques d'un projet d'EMR.

2 Calcul des risques résiduels

2.1 Généralités

Risque résiduel (residual risk) – Risque qui demeure une fois les mesures de protection sélectionnées, approuvées et mises en œuvre.

Nouvelle définition.

À l'achèvement des phases d'identification et d'évaluation des biens et d'évaluation des menaces et du volet d'évaluation des vulnérabilités de la phase d'évaluation des risques d'un projet d'EMR, on a attribué aux trois variables de risque (valeurs des biens, menaces et vulnérabilités) une cote allant de Très faible à Très élevée. Dans le cadre du deuxième volet de la phase d'évaluation des risques, ces trois facteurs sont combinés afin de cerner les risques résiduels et d'en déterminer l'ordre de priorité; les risques résiduels sont les risques qui demeurent une fois mises en œuvre les mesures de protection proposées et approuvées.

2.2 Calcul de base des risques

À cette étape d'un projet d'EMR, tous les biens inclus dans la portée de l'évaluation ont été identifiés et se sont vu attribuer une cote en fonction des dommages auxquels on peut raisonnablement s'attendre en cas de compromission de la confidentialité, de la disponibilité ou de l'intégrité. Les menaces connexes qui peuvent toucher les biens ont été cotées en fonction de leur probabilité d'occurrence et de la gravité éventuelle des conséquences. On a attribué aux

vulnérabilités connexes susceptibles de causer des préjudices aux biens une cote relative fondée sur leur incidence sur la probabilité de compromission et la gravité des conséquences.
Dans le cadre de l'analyse, on a affecté à chacune des trois variables un niveau allant de Très faible à Très élevée. Maintenant, pour déterminer le risque résiduel découlant d'une menace exploitant une vulnérabilité connexe en vue de compromettre un bien, il faut attribuer à ces trois variables une cote numérique entre 1 et 5, en fonction du tableau E-1 ci-dessous.

Niveau de la valeur du bien, des menaces et des vulnérabilités	Très faible	Faible	Moyen	Élevé	Très élevé
Cote de calcul du risque	1	2	3	4	5

Tableau E-1 : Cotes numériques – Niveaux de la valeur du bien, des menaces et des vulnérabilités

Comme l'illustre la figure E-1, les risques résiduels évalués correspondent au produit des trois variables pour chaque combinaison d'un bien, d'une menace connexe et de la vulnérabilité associée provenant du tableau d'évaluation des vulnérabilités (tableau D-5) de l'appendice D-4.

Risque résiduel = Valeur du bien × Menace × Vulnérabilité

Figure E-1 : Calcul du risque résiduel

Compte tenu du fait qu'une cote numérique entre 1 et 5 est attribuée à chaque variable, la cote finale du risque résiduel peut se trouver entre 1 et 125.

2.3 Niveaux de risque

Même si les cotes brutes peuvent immédiatement servir à établir l'ordre de priorité des risques résiduels, il est souvent utile de regrouper les résultats similaires dans des gammes allant de Très faible à Très élevé. Les seuils situés entre les cotes Moyen, Élevé et Très élevé figurant au tableau E-2 ont été sélectionnés en fonction de l'hypothèse sous-jacente que lorsque deux des trois variables obtiennent la même cote, par exemple Moyen, et que la troisième se trouve dans la catégorie supérieure suivante, dans ce cas Élevé, il semble prudent d'adopter une cote globale correspondant à la cote la plus élevée. Les limites entre les cotes Très faible, Faible et Moyen ont été légèrement ajustées à la hausse, afin d'obtenir une répartition plus uniforme des résultats. Comme l'indique le tableau E-2, la gamme correspondant à la cote Moyen constitue le groupe le plus important (43 combinaisons possibles), alors qu'on compte un nombre de combinaisons légèrement inférieur dans les gammes Élevé et Faible, et encore moins dans les gammes Très élevé et Très faible. Enfin, les tableaux E1-3 à E1-7 présentent une ventilation complète de tous les résultats possibles pour chaque combinaison de valeurs de bien, de menaces et de vulnérabilités.

Note de base du risque	1-4	5-12	15-32	36-75	80-125
Niveau de risque	Très faible	Faible	Moyen	Élevé	Très élevé
Nombre de résultats dans la gamme	13	34	43	28	7

Tableau E-2 : Niveaux et gammes de risques

2.4 Application pratique

2.4.1 Généralités

Pour obtenir des résultats plus réalistes, le calcul direct du risque résiduel comme produit de trois variables (valeur du bien, menace et vulnérabilité) doit être raffiné par la prise en compte de certaines données pratiques, dans certaines circonstances.

2.4.2 Valeurs marginales

Lorsque deux variables ou plus tombent à la limite supérieure ou inférieure de la gamme pour les valeurs évaluées, il est généralement prudent de diminuer ou d'augmenter le niveau d'un facteur pour mieux refléter le risque réel. Par exemple, si une cote Moyen est attribuée à la valeur d'un bien en raison d'une perte financière prévue de 9,8 millions de dollars en cas de compromission, les dommages estimatifs se trouvent très près de la limite entre les cotes Moyen et Élevé des valeurs du bien et doivent donc être marquées à la hausse (↑), conformément aux directives énoncées à l'appendice B-4, Tableau détaillé des préjudices. Si une menace ou une vulnérabilité connexe, ou les deux, se voient également attribuer une cote se trouvant à la limite supérieure de l'échelle, à cheval entre deux gammes, l'une des trois variables (généralement celle qui a la cote la plus faible) doit être majorée d'un échelon aux fins du calcul du risque résiduel; cette majoration doit être consignée comme il se doit dans l'évaluation finale des risques.

2.4.3 Valeurs incertaines

Il peut arriver, en dépit des efforts des membres de l'équipe de l'EMR visant à atteindre un consensus à propos des cotes réalistes pour les valeurs des biens, les menaces et les vulnérabilités, que surviennent des différends légitimes. Dans d'autres cas, notamment en ce qui a trait aux menaces et aux vulnérabilités, les cotes appropriées peuvent être difficiles à établir à cause de données incomplètes ou contradictoires. Au lieu de forcer l'évaluation pour obtenir une cote unique, il est généralement préférable de calculer le risque résiduel à l'aide des deux valeurs contradictoires. Par exemple, il est possible que, d'après les renseignements dont on dispose, il soit difficile de déterminer si un agent de menace délibérée a des connaissances, des compétences et des ressources considérables ou simplement ordinaires; dans un tel cas, la cote (risque élevé ou moyen) à attribuer à la capacité de l'agent de menace, et par conséquent, la cote à attribuer à l'incidence ou à la gravité, ne sont pas claires. Compte tenu de cette incertitude, deux valeurs doivent être calculées pour le risque résiduel évalué, à l'aide de la cote supérieure et de la cote inférieure attribuées à la menace.

2.4.4 Menaces délibérées

La probabilité d'occurrence de bon nombre de menaces, notamment des accidents et des sinistres naturels, demeure relativement constante, du moins à court terme. Il va de soi que des changements peuvent survenir, mais en règle générale, ils se produisent plutôt graduellement. Par exemple, la probabilité d'occurrence de certains sinistres naturels, comme un ouragan, s'est accrue considérablement au cours des 50 dernières années, en partie à cause du réchauffement de la planète. Comme la plupart des projets d'EMR sont actualisés périodiquement, il est peu probable que les variations à long terme de cette nature aient des effets sur les constatations relatives à la période visée par un rapport d'EMR, quel qu'il soit. Au contraire, la probabilité d'occurrence de nombreuses menaces délibérées peut être beaucoup plus volatile, puisque les intentions des agents de menace peuvent changer très rapidement, pratiquement du jour au lendemain. À ce jour, les cas d'extorsion visant la récupération de fichiers de données chiffrées sont chose assez courante dans certains pays, alors qu'ils sont pratiquement inconnus au Canada. La probabilité de réalisation de la menace serait donc cotée Faible ou Moyenne à l'occasion de la phase d'évaluation des menaces, conformément au tableau C-1. Si toutefois la situation changeait, la probabilité et la menace globale pourraient augmenter rapidement, sans préavis, avant que des mesures de protection appropriées ne puissent être mise en œuvre. Par conséquent, lorsque les intentions d'un agent de menace délibérée sont considérées comme une menace faible ou moyenne, il est prudent de calculer deux risques résiduels, un en fonction des intentions et des capacités actuelles, et le deuxième à un échelon supérieur en fonction d'une probabilité élevée. Si les deux niveaux de risque varient considérablement, l'écart peut être consigné à la phase des recommandations du projet d'EMR pour justifier des mesures de protection supplémentaires avant que le changement ne se produise.

3 Liste priorisée des risques résiduels évalués

Comme il en est question ci-dessus, les risques résiduels peuvent être calculés en fonction de trois éléments, soit les valeurs du bien, les menaces connexes et les vulnérabilités associées. Comme une même menace peut toucher plusieurs biens et valeurs des biens, et qu'une même vulnérabilité peut exposer de nombreux biens à des menaces diverses, la liste des risques résiduels peut se révéler très longue, même pour un projet d'EMR très ciblé. Par conséquent, pour obtenir des résultats plus faciles à gérer, les biens et les menaces, en particulier, sont respectivement rassemblés en groupes et en sous-groupes, et en fonction de l'activité de la catégorie d'agents de menace. Cette information doit être consignée dans la liste des risques résiduels, qui constitue le résultat final du volet du calcul des risques résiduels de la phase d'évaluation des risques d'un projet d'EMR. Le simple tri en fonction du niveau du risque résiduel évalué (de Très faible à Très élevé) ou des cotes brutes (de 1 à 125) permet d'établir rapidement l'ordre de priorité de chacun des risques et de repérer ceux qui sont les plus inquiétants.

La liste des risques résiduels évalués est illustrée au tableau E-3, et des renseignements supplémentaires sont fournis à l'appendice E-2.

Bien (Groupe/ Sous-groupe)	Valeurs du bien			Menace connexe (Activité/catégorie d'agent)	M	Vulnérabilité connexe	V	Risque résiduel ($B_{Val} \times M \times V$)	R
	C	D	I						

Tableau E-3: Liste des risques résiduels évalués

Page intentionnellement laissée en blanc

Appendice E-1 - Tableaux des risques résiduels

1 Instructions

Après avoir terminé la Phase d'identification et d'évaluation des biens, la Phase d'évaluation des menaces et le segment d'évaluation des vulnérabilités de la Phase d'évaluation des risques d'un projet d'EMR, on peut calculer les risques résiduels et leur attribuer des niveaux appropriés, comme suit :

- **Étape 1a.** Pour tous les biens inclus dans la portée de l'évaluation, convertir les valeurs de Très faible à Très élevé, saisies dans le tableau d'évaluation des biens/énoncé de sensibilité de l'appendice B-5, en une cote brute de un à cinq conformément au tableau E1-1 ci-dessous et entrer les résultats dans les colonnes pertinentes de la liste des risques résiduels évalués de l'appendice E-2.
- **Étape 1b.** Si les valeurs de bien attribuées se rapprochent de la ligne de démarcation entre deux niveaux, baliser les entrées en conséquence en utilisant soit ↑ ou ↓ pour indiquer leur position dans la gamme supérieure ou inférieure du spectre, respectivement.
- **Étape 2a.** Pour toutes les menaces associées à chaque bien, convertir les niveaux de Très faible à Très élevé, saisis dans le tableau d'évaluation des menaces de l'appendice C-4, en une cote brute de un à cinq conformément au tableau E1-1 ci-dessous et entrer les résultats dans les colonnes pertinentes de la liste des risques résiduels évalués de l'appendice E-2.
- **Étape 2b.** Si les menaces évaluées se rapprochent de la ligne de démarcation entre deux niveaux, baliser les entrées en conséquence en utilisant soit ↑ ou ↓ pour indiquer leur position dans la gamme supérieure ou inférieure du spectre, respectivement.
- **Étape 2c.** S'il y a une évidence contradictoire concernant les niveaux de menace, entrer les deux valeurs, élevée et faible, sur des lignes séparées.
- **Étape 2d.** Dans le cas des menaces délibérées qui ont un niveau de probabilité d'occurrence de Faible ou Moyen, considérer l'incidence potentielle du changement d'intentions de l'agent de menace en recalculant le niveau global de menace à l'aide du tableau C-3, Tableau des niveaux de menace, en utilisant un niveau de probabilité Élevé plutôt que Faible ou Moyen, et saisir les résultats comme deuxième entrée.
- **Étape 3a.** Pour toutes les vulnérabilités qui exposent les biens à des menaces, convertir les niveaux de Très faible à Très élevé, saisis dans le Tableau des évaluation des vulnérabilités de l'appendice D-4, en une cote brute de un à cinq conformément au tableau E1-1 ci-dessous et entrer les résultats dans les colonnes pertinentes de la liste des risques résiduels de l'appendice E-2.
- **Étape 3b.** Pour les vulnérabilités qui se rapprochent de la ligne de démarcation entre deux niveaux, baliser les entrées en conséquence en utilisant soit ↑ ou ↓ pour indiquer leur position dans la gamme supérieure ou inférieure du spectre, respectivement.
- **Étape 3c.** En cas de doute concernant les niveaux de vulnérabilité, entrer les deux valeurs, élevée et faible, sur des lignes séparées.

Niveau de la valeur du bien, des menaces et des vulnérabilités	Très faible	Faible	Moyen	Élevé	Très élevé
Cote de calcul du risque	1	2	3	4	5

Tableau E1-1 : Cotes numériques – Niveaux de la valeur du bien, des menaces et vulnérabilités

- **Étape 4a.** Après avoir entré tous les biens, les menaces et les vulnérabilités connexes dans la liste des risques résiduels évalués de l'appendice E-2 ainsi que les cotes numériques obtenues de leurs niveaux, on peut calculer le produit des trois variables et l'entrer soit comme cote brute de 1 à 125 ou comme niveau de risque pertinent selon le tableau E1-2 ci-dessous.
- **Étape 4b.** Si deux ou trois des facteurs de risque tombent à la limite supérieure ou inférieure de la gamme de leurs niveaux évalués, augmenter ou réduire d'un niveau la note brute de la variable cotée la plus faible avant de calculer le risque résiduel. Cette étape peut être omise lorsqu'une ou deux des variables se situent à une extrémité du spectre et une autre à l'extrémité opposée, s'annulant ainsi l'une l'autre.

Note de base du risque	1-4	5-12	15-32	36-75	80-125
Niveau de risque	Très faible	Faible	Moyen	Élevé	Très élevé
Nombre de résultats dans la gamme	13	34	43	28	7

Tableau E1-2 : Niveaux et gammes de risques

2 Tableaux détaillés d'évaluation des risques

Les tableaux E1-3 à E1-7 offrent une ventilation de tous les résultats possibles du calcul du risque résiduel évalué. Sélectionnez simplement le tableau de la valeur de bien concernée et déterminez le risque résiduel en corrélant le niveau de menace connexe sur l'axe horizontal avec le niveau de vulnérabilité connexe sur l'axe vertical.

Niveau de vulnérabilité	**Niveau de menace**				
	Très faible	Faible	Moyen	Élevé	Très élevé
Très faible	TF	TF	TF	TF	F
Faible	TF	TF	F	F	F
Moyen	TF	F	F	F	M
Élevé	TF	F	F	M	M
Très élevé	F	F	M	M	M

Tableau E1-3: Tableau des risques pour les valeurs de bien très faibles

Niveau de vulnérabilité	Niveau de menace				
	Très faible	Faible	Moyen	Élevé	Très élevé
Très faible	TF	TF	F	F	F
Faible	TF	F	F	M	M
Moyen	F	F	M	M	M
Élevé	F	M	M	M	E
Très élevé	F	M	M	E	E

Tableau E1-4 : Tableau des risques pour les valeurs de bien faibles

Niveau de vulnérabilité	Niveau de menace				
	Très faible	Faible	Moyen	Élevé	Très élevé
Très faible	TF	F	F	F	M
Faible	F	F	M	M	M
Moyen	F	M	M	E	E
Élevé	F	M	E	E	E
Très élevé	M	M	E	E	E

Tableau E1-5: Tableau des risques pour les valeurs de bien moyennes

Niveau de vulnérabilité	Niveau de menace				
	Très faible	Faible	Moyen	Élevé	Très élevé
Très faible	TF	F	F	M	M
Faible	F	M	M	M	E
Moyen	F	M	E	E	E
Élevé	M	M	E	E	TE
Très élevé	M	E	E	TE	TE

Tableau E1-6: Tableau des risques pour les valeurs de bien élevées

Niveau de vulnérabilité	Niveau de menace				
	Très faible	Faible	Moyen	Élevé	Très élevé
Très faible	F	F	M	M	M
Faible	F	M	M	E	E
Moyen	M	M	E	E	E
Élevé	M	E	E	TE	TE
Très élevé	M	E	E	TE	TE

Tableau E1-7: Tableau des risques pour les valeurs de bien très élevées

3 Exemple

3.1 Entrepôt de médicaments régional

Un entrepôt de médicaments régional contient 12 millions de dollars de morphine; pour calculer le risque résiduel évalué, on peut déterminer les variables de risque, comme suit :

- **Évaluation du bien.** La valeur principale du bien dans ce cas doit refléter le préjudice auquel on doit vraisemblablement s'attendre dans l'éventualité où les médicaments sont perdus ou volés; cette préoccupation se situe au plan de la disponibilité. L'incidence psychologique d'une perte accidentelle peut être très minime; par contre, le vol de médicaments dans une installation publique est beaucoup plus susceptible de soulever de sérieux doutes et de l'incertitude dans le public en général; la valeur du bien dans ce cas se situe probablement au niveau Moyen, conformément au tableau détaillé des préjudices à l'appendice B-4. Dans l'éventualité où la morphine n'est plus disponible pour quelque raison que ce soit, l'incidence sur certains patients pourrait être très dévastatrice et entraîner des difficultés physiques graves pour au moins certains, sinon plusieurs, d'entre eux; de toute évidence, la valeur du bien dans ce cas peut se situer au niveau Moyen et, même fort probablement, au niveau Élevé. Enfin, du point de vue financier, le coût de remplacement complet du stock peut s'élever jusqu'à 12 millions de dollars; dans ce cas, la valeur de disponibilité se situe dans la gamme inférieure du niveau Élevé et peut être donc être balisée par le symbole (↓).
- **Évaluation des menaces.** Bien que des gangs de motards criminalisés n'aient jamais dévalisé un entrepôt de médicaments régional par le passé, ils se sont introduits en moyenne une fois tous les 90 jours dans des pharmacies de quartier pour voler des médicaments. Dans ce cas, on peut donc, en utilisant la colonne 3 du tableau C3-1, Tableau des probabilités des menaces, coter la probabilité de la menace au niveau Moyen, quoique à l'extrémité inférieure de la gamme, vue la fréquence passée de 10 à 100 jours pour des biens similaires d'origines différentes. Compte tenu des connaissances, des compétences et des ressources à la disposition de tels gangs, les capacités d'agent de menace sont sans aucun doute d'un niveau Élevé; le niveau global de menace doit donc être coté Élevé, conformément au tableau C3-3. Puisque la fréquence réelle d'une fois tous les 90 jours se situe à l'extrémité inférieure de la gamme, on peut également baliser le niveau de menace en utilisant le symbole (↓).
- **Évaluation des vulnérabilités.** Un bâtiment à ossature de bois et placage de brique offre peu de résistance à une invasion par la force, même si ses fenêtres sont bardées de grillages en acier et ses murs renforcés de contreplaqué; dans ce cas, l'incidence sur la probabilité de compromission doit être cotée au niveau Élevé, conformément au tableau D3-1, Incidence des vulnérabilités sur la prévention. Même si un système d'alarme anti-intrusion d'excellente qualité a été installé pour avertir la police locale d'une entrée non autorisée, cette dernière n'intervient normalement pas avant vingt minutes ou plus. Dans les faits, un excellent mécanisme de détection est miné par une capacité d'intervention relativement lente. À l'aide du tableau D3-2, Incidence des vulnérabilités sur la détection, la réaction ou la reprise, on peut attribuer à cette faiblesse un niveau Moyen puisque les mesures de protection ne sont que modérément efficaces. Puisque les faiblesses de prévention liées à l'intégrité de la structure et les faiblesses de

réaction liées à la force policière sont clairement intereliées, on doit effectuer une évaluation approfondie de la vulnérabilité, conformément à la section 6.1.3 de l'annexe D, pour attribuer au niveau de vulnérabilité la cote Élevé.

- **Évaluation des risques.** Dans cet exemple, on a attribué aux trois variables de risque (valeur du bien, menace et vulnérabilité) le niveau Élevé pour obtenir un risque résiduel de 64 (4×4×4). D'autre part, la valeur du bien et la menace se situent à l'extrémité inférieure de la gamme Élevé; on doit donc ajuster le risque résiduel évalué en conséquence et réduire d'un niveau la variable de valeur inférieure pour obtenir un résultat de 48 (3×4×4). Malgré cet ajustement, les deux résultats indiquent un niveau de risque résiduel Élevé.

Page intentionnellement laissée en blanc

Appendice E-2 – Liste des risques résiduels évalués

Bien (Groupe/ sous-groupe)	Valeurs du bien			Menace connexe (Activité/catégorie d'agent)	M	Vulnérabilité connexe	V	Risque résiduel ($B_{Val} \times M \times V$)	R
	C	D	I						

1 Instructions

En utilisant les résultats de la Phase d'identification des biens, de la Phase d'évaluation des menaces et du segment d'évaluation des vulnérabilités de la Phase d'évaluation des risques, plus particulièrement le tableau d'évaluation des biens/énoncé de sensibilité, le tableau d'évaluation des menaces et le tableau d'évaluation des vulnérabilités des appendices B-5, C-4 et D-4, respectivement :

- **Étape 1.** Inscrire tous les biens inclus dans la portée de l'évaluation dans la première colonne en utilisant des entrées séparées pour chaque valeur de bien concernée et en indiquant celles qui se situent près des limites inférieures ou supérieures du niveau de préjudice.
- **Étape 2.** Inscrire toutes les menaces connexes susceptibles de compromettre ces biens et valeurs de bien dans la cinquième colonne et leurs niveaux dans la sixième, en indiquant celles qui se situent près des limites inférieures ou supérieures du niveau évalué. S'il y a une évidence contradictoire concernant le niveau de menace réel, entrer deux entrées distinctes pour les valeurs supérieures et inférieures. Dans le cas des menaces délibérées pour lesquelles le niveau des intentions de l'agent de menace (c.-à-d., la probabilité des menaces) est coté Moyen ou Faible, insérer une autre ligne pour refléter le niveau supérieur de la menace advenant que le niveau des intentions de l'agent passe à Élevé.
- **Étape 3.** Inscrire toutes les vulnérabilités connexes qui exposent chaque bien à une menace connexe dans la septième colonne et leurs niveaux dans la huitième, en indiquant celles qui se situent près des limites inférieures ou supérieures du niveau évalué. S'il y a une évidence contradictoire concernant le niveau de vulnérabilité réel, inclure des entrées distinctes pour les valeurs supérieures et inférieures.
- **Étape 4.** Convertir les niveaux attribués à chacune des trois variables (valeurs de bien, menaces et vulnérabilités) en cote numérique de 1 à 5, calculer le produit et entrer les résultats dans la neuvième colonne. Dans les cas où deux ou trois des facteurs se situent dans la gamme supérieure ou inférieure du niveau évalué, ajuster la cote inférieure de 1 vers le haut ou vers le bas pour le calcul du risque résiduel. Enfin, on peut insérer le niveau de risque correspondant, de Très faible à Très élevé, dans la dixième colonne.

2 Exemple

L'exemple utilisé à l'appendice E-1, concernant un entrepôt de médicaments régional, produit l'entrée ci-dessous dans la liste des risques résiduels :

Bien (Groupe/ sous-groupe)	Valeurs du bien			Menace connexe (Activité/Catégorie d'agent)	M	Vulnérabilité connexe	V	Risque résiduel ($B_{Val} \times M \times V$)	R
	C	D	I						
Médicaments/Morphine		E↓		Gangs de motards/Vol	E↓	Intégrité structurelle Intervention lente	E	$(4\text{-}1)^1 \times 4 \times 4 = 48$	E

[1] La valeur du bien et le niveau de menace ont été évalués à l'extrémité inférieure de la gamme Élevé (E↓); la valeur la plus faible est donc réduite de 1 pour le calcul du risque résiduel. Dans ce cas particulier, la valeur du bien ou le niveau de menace peut avoir été ajusté puisque les deux variables ont la même valeur.

Page intentionnellement laissée en blanc

Annexe F – Phase des recommandations

1 Introduction

1.1 Généralités

La phase des recommandations d'un projet d'EMR comprend quatre processus séquentiels et un résultat important, soit :

- **Identification des risques inacceptables** — déterminer lesquels des risques résiduels évalués durant la phase d'évaluation des risques d'un projet d'EMR dépassent le niveau de risque cible spécifié dans le plan de travail de l'EMR;[1]
- **Sélection des mesures de protection possibles —** identifier un ensemble de mesures de protection appropriées qui pourraient atténuer les risques résiduels inacceptables et les ramener à un niveau acceptable;
- **Calcul des coûts —** évaluer le coût et la rentabilité des mesures de protection proposées;
- **Évaluation des risques résiduels projetés** — prévoir les risques résiduels qui restent après l'approbation et la pleine mise en œuvre des mesures de protection recommandées;
- **Rapport d'EMR final —** présenter les conclusions et recommandations du projet d'EMR au responsable de l'acceptation des risques.

1.2 But

Le but de cette annexe est de décrire les quatre processus et le résultat unique de la phase des recommandations d'un projet d'EMR.

2 Identification des risques inacceptables

2.1 Généralités

Une fois que les risques résiduels ont été calculés et priorisés durant la quatrième phase de l'évaluation, l'équipe d'EMR doit généralement concentrer ses efforts sur ceux qui dépassent le seuil cible défini dans le plan de travail original de l'EMR et approuvé par le responsable de l'acceptation des risques. Elle pourra ensuite examiner les différentes options en détail afin de pouvoir recommander des mesures de protection appropriées qui permettront aux cadres supérieurs d'assumer une position de risque acceptable à un coût abordable.

[1] Comme il est indiqué à la **section 5 de l'appendice A-6**, **Exemple de plan de travail de l'EMR**, le niveau de risque cible doit être identifié explicitement avant chaque projet d'EMR.

2.2 Déterminants sous-jacents

Le niveau de risque réel acceptable varie selon les organismes en fonction de plusieurs facteurs, y compris :

- **Culture organisationnelle.** Certains organismes et particuliers ont une plus grande tolérance à l'égard du risque, surtout en raison de leur expérience antérieure et de leurs préférences personnelles. Ces facteurs doivent être rationalisés dans la mesure du possible, mais ils ne peuvent pas être complètement éliminés.
- **Obligations réglementaires et imposées par la loi.** Pour certains services et secteurs d'activité gouvernementaux, les niveaux de risque acceptables peuvent être régis, du moins indirectement, par les lois fédérales. Par exemple, la *Loi sur la protection des renseignements personnels* et ses règlements d'application exigent la protection des renseignements personnels.
- **Possibilités.** Dans certains cas, on peut accepter des risques plus élevés afin d'accroître les avantages découlant des possibilités offertes par certains programmes ou projets. Par exemple, les risques inhérents au recours à Internet pour la prestation des services électroniques sont souvent compensés par les avantages correspondants (réduction des coûts et plus grande commodité pour les clients).
- **Commodité opérationnelle.** Il est parfois impossible de ramener les risques résiduels évalués à un niveau acceptable parce qu'il n'existe pas de mesures de protection appropriées ou qu'elles ne peuvent pas être mises en œuvre en temps opportun. En pareilles circonstances, il pourrait être nécessaire, pour atteindre des objectifs opérationnels essentiels, d'accepter des niveaux de risque par ailleurs intolérables à court ou à long terme.
- **Contraintes de coût.** D'un point de vue pratique, les mesures de protection requises pour maintenir un niveau acceptable de risque résiduel pouvant être extrêmement coûteuses, il pourrait être nécessaire d'approuver des risques accrus, bien qu'avec de sérieuses réserves.

2.3 Gammes de risques

Malgré l'influence possible de chacun des facteurs mentionnés plus haut sur l'évaluation des risques résiduels, une approche commune de la détermination de l'acceptabilité est généralement préférable afin d'accroître l'interopérabilité et les communications entre les différents programmes et projets d'EMR. Compte tenu de cet objectif, la division des valeurs possibles de risque en cinq catégories allant de Très faible à Très élevé peut faciliter la prise des décisions. En règle générale, les risques résiduels classés dans la catégorie Très élevé sont tout à fait inacceptables et nécessitent des mesures correctives. À l'autre extrémité du spectre, les risques de niveau Très faible sont tout à fait acceptables et n'exigent aucun suivi. Bien qu'une analyse plus poussée puisse être requise, les risques résiduels élevés sont probablement inacceptables, tandis que les risques faibles sont probablement acceptables. Les risques de niveau Moyen sont plus difficiles à jauger et exigent un examen très prudent afin de déterminer leur acceptabilité relative.

Cette progression logique est illustrée au tableau F-1.

Risque résiduel évalué	Très faible	Faible	Moyen	Élevé	Très élevé
Acceptabilité	Tout à fait acceptable	Probablement acceptable	Peut-être inacceptable	Probablement inacceptable	Tout à fait inacceptable

Tableau F-1 : Acceptabilité des risques résiduels évalués

2.4 Options de gestion

2.4.1 Généralités

De toute évidence, les recommandations du rapport d'EMR final peuvent varier considérablement selon les niveaux de risque relatifs et particulièrement selon le degré d'acceptabilité des risques résiduels évalués.

2.4.2 Risques résiduels acceptables

Dans le cas des risques acceptables, généralement classés dans les catégories Très faible, Faible et parfois Moyen, les gestionnaires responsables peuvent avoir à choisir entre les options suivantes :

- **Conserver les mesures de protection existantes.** Les mesures de protection existantes qui ramènent le risque résiduel à un niveau acceptable doivent être conservées, sauf si d'autres options permettent d'atteindre les mêmes objectifs à meilleur marché. Bien sûr, les mesures de protection existantes qui ne contribuent pas à une réduction substantielle des risques doivent être signalées en vue de leur élimination éventuelle.
- **Mettre en œuvre les mesures de protection proposées.** Les mesures de protection proposées pour atteindre un niveau acceptable de risque résiduel qui sont prises en compte dans l'EMR doivent être approuvées, financées, installées et testées afin d'en vérifier l'efficacité.
- **Éliminer les mesures de protection excessives.** Dans quelques cas, lorsque les risques résiduels ont été ramenés bien en-deçà du seuil acceptable, c'est-à-dire au niveau Faible ou Très faible, grâce à des mesures de protection coûteuses ou peu pratiques, il peut être possible de recommander l'élimination de ces mesures afin d'accroître les économies ou les gains d'efficacité, à condition que les risques connexes ne s'écartent pas de la fourchette acceptable (habituellement les niveaux Faible ou Moyen).

2.4.3 Risques résiduels inacceptables

Dans le cas des risques résiduels inacceptables, généralement aux niveaux Très élevé, Élevé et parfois Moyen, n'importe quelle combinaison des options suivantes peut être recommandée aux responsables :

- **Proposer des mesures de protection additionnelles.** Dans la plupart des cas, l'équipe d'EMR recommandera des mesures de protection additionnelles afin de réduire

les valeurs des biens, les menaces ou, plus souvent, les vulnérabilités et d'assurer ainsi des niveaux acceptables de risque résiduel.

- **Réviser les exigences originales.** Parfois, lorsque les mesures de protection appropriées sont extrêmement coûteuses, peu pratiques sur le plan technique ou simplement indisponibles, il peut être nécessaire de revoir le projet ou le système dans son ensemble afin :
  - de réviser les exigences originales et de limiter les valeurs des biens,
  - de choisir un emplacement plus sécurisé,
  - d'adopter une architecture plus robuste, ou
  - d'accepter un niveau plus élevé de risque résiduel.
- **Rejeter la proposition ou annuler le projet.** Dans les rares cas où les risques résiduels sont complètement inacceptables, l'équipe d'EMR pourrait avoir à recommander le rejet de la proposition ou l'annulation du projet selon l'objet de l'évaluation.

2.5 Fondement des recommandations

Dans le cadre de l'évaluation des vulnérabilités (annexe D), les mesures de protection existantes et proposées ont été identifiées et classées selon leurs fonctions de sécurité, à savoir l'évitement, la dissuasion, la prévention, la détection, l'intervention ou la reprise. Puis, pour déterminer les vulnérabilités relatives, on a évalué l'efficacité de ces mesures de protection en fonction de leur incidence sur trois facteurs : 1) la probabilité d'occurrence d'une menace; 2) la probabilité de compromission au cas où la menace se réaliserait; 3) la gravité des conséquences ou l'ampleur des préjudices probables.[2] Étant donné la relation inverse qui existe entre les vulnérabilités et l'efficacité des mesures de protection, des solutions rentables permettant d'atténuer les risques résiduels inacceptables pourraient être recommandées au cours des trois processus suivants de la phase des recommandations :

- **Sélection des mesures de protection.** Déterminer quelles mesures de sécurité pourraient être mises en œuvre afin d'atténuer les risques inacceptables en se fondant sur des critères de sélection explicites.
- **Estimation des coûts.** Évaluer les coûts et la rentabilité de chaque option.
- **Risque résiduel projeté.** Calculer le risque résiduel projeté une fois que les recommandations auront été approuvées et mises en œuvre.

3 Sélection des mesures de protection potentielles

3.1 Généralités

La Liste des risques résiduels évalués établie à la fin de la phase d'évaluation des risques d'un projet d'EMR, illustrée à l'appendice E-2, est à la fois un point de départ logique et un outil précieux pour le choix des mesures de protection aptes à atténuer les risques inacceptables. Cependant, pour que les résultats soient cohérents, l'analyse étayant les recommandations du rapport final sur l'EMR doit se fonder sur plusieurs critères de sélection explicites, de nature

[2] Voir la **section 2**, **Recensement des mesures de protection**, et la **section 3**, **Efficacité des mesures de protection**, de l'**annexe D**, **Évaluation des vulnérabilités**.

qualitative ou quantitative selon le cas. Ces critères de sélection fournissent une justification objective pour chaque mesure de protection en tenant compte des variables de risque et de l'efficacité globale des mesures de sécurité proposées pour les atténuer.

3.2 Critères de sélection des mesures de protection : Variables de risque

3.2.1 Biens protégés

Comme il est indiqué à l'appendice F-2, Liste des mesures de protection, certaines mesures de sécurité protègent différentes catégories de biens tandis que d'autres couvrent seulement quelques groupes ou sous-groupes à l'intérieur d'une seule catégorie de biens. Ce facteur doit être pris en considération dans le choix des contre-mesures appropriées, et ce, pour deux raisons. Premièrement, les mesures de protection recommandées doivent protéger tous les biens qui présentent des risques résiduels inacceptables. Pour identifier ces biens, il suffit de trier les éléments de la liste des risques résiduels évalués par niveau de risque, de Très élevé à Très faible, et d'examiner les biens correspondants de la première colonne. Deuxièmement, toutes choses étant égales par ailleurs, les mécanismes de sécurité qui protègent de multiples biens sont préférables à ceux dont l'effet est plus limité parce qu'ils peuvent atténuer un plus grand nombre de risques.

3.2.2 Valeurs des biens préservées

Un examen des valeurs des biens (confidentialité, disponibilité et intégrité) exposées aux plus grands risques est un prolongement logique du premier critère de sélection. De toute évidence, les mesures de protection doivent être choisies afin de protéger non seulement les biens mais aussi les valeurs des biens qui contribuent aux risques résiduels inacceptables. Cet examen est utile, car certaines mesures de protection peuvent être contre-productives dans certaines circonstances, étant donné la tension inhérente entre les mécanismes de confidentialité et de disponibilité. Par exemple, le chiffrement des fichiers, une mesure de confidentialité, ne sert pas à grand-chose lorsque la disponibilité est la principale considération. Pis encore, il pourrait nuire à l'échange des données et donc à la disponibilité.

3.2.3 Activités de menace modérées

Comme il est noté à la section 3.3 de l'annexe D, Évaluation des vulnérabilités, la plupart des mesures de protection atténuent le risque en réduisant les vulnérabilités plutôt que les menaces. Cela dit, toutes les menaces qui présentent des risques résiduels inacceptables doivent être explicitement identifiées pour que les mesures de protection proposées s'y attaquent directement ou, plus souvent, indirectement en atténuant les vulnérabilités correspondantes. Là encore, on peut identifier ces menaces en triant les éléments de la liste des risques résiduels évalués par niveaux de risque. Enfin, les mesures de protection qui atténuent de multiples menaces sont préférables à celles dont l'effet est plus ciblé parce qu'elles peuvent s'attaquer à différents risques.

3.2.4 Vulnérabilités atténuées

De même, les mesures de protection doivent être choisies de manière à atténuer les vulnérabilités associées aux risques résiduels inacceptables. Comme dans le cas des biens protégés et des

menaces atténuées, les mesures de sécurité qui s'attaquent à plusieurs vulnérabilités sont généralement préférables.

3.2.5 Fonctions de sécurité exécutées

Les fonctions de sécurité assurées par différentes mesures de protection (évitement, dissuasion, prévention, détection, réaction et reprise) et leur incidence sur les variables de risque (valeurs des biens, menaces et vulnérabilités) sont examinées en détail à la section 3 de l'annexe D, Évaluation des vulnérabilités. Il faut tenir compte de ces fonctions lorsqu'on choisit les mesures de sécurité, car aucune mesure de protection n'est infaillible. Ainsi, les recommandations finales d'un rapport d'EMR doivent généralement refléter une approche équilibrée combinant des mécanismes liés de détection, de réaction et de reprise avec des mesures d'évitement, de dissuasion et, plus fréquemment, de prévention afin d'assurer une défense en profondeur grâce à une stratégie de sécurité active, illustrée à la Figure F-1. Dans certains cas, par exemple lorsqu'il est impossible d'éviter ou de prévenir un sinistre naturel, il faut accorder une plus grande priorité aux méthodes de détection précoce, de réaction et de reprise. Par ailleurs, la prévention peut prendre plus d'importance lorsque la confidentialité est la principale considération, simplement parce qu'il peut être difficile, sinon impossible, de se remettre d'une compromission et de rétablir le secret original en cas de divulgation non autorisée. Enfin, toutes les mesures de détection doivent avoir des mécanismes correspondants de réaction et probablement de reprise.

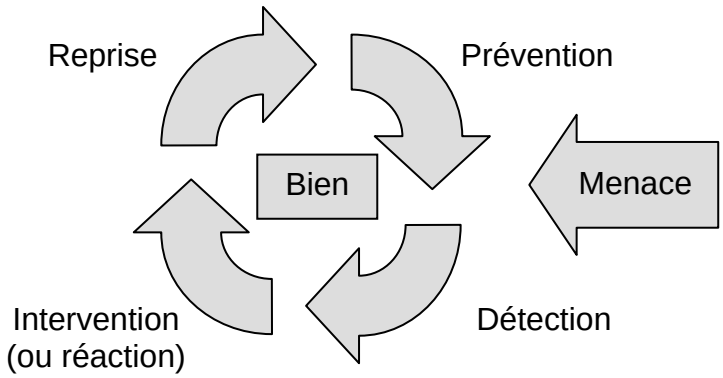

Figure F-1 : Stratégie de sécurité active

3.3 Critères de sélection des mesures de protection : Efficacité des mesures de protection

3.3.1 Considérations de base

Comme il est noté plus haut, les mesures de protection qui peuvent être prises pour remédier aux risques inacceptables sont identifiées dès la première étape du processus de sélection en fonction de leur capacité à : 1) protéger les biens et les valeurs des biens exposés aux plus grands risques; 2) atténuer les plus graves menaces; 3) atténuer les plus graves vulnérabilités; 4) maintenir un équilibre entre l'évitement, la dissuasion ou la prévention, d'une part, et la détection, l'intervention et la reprise, d'autre part. Durant la deuxième étape, l'efficacité des différentes options est évaluée en fonction de leur incidence sur les trois variables de risque : les valeurs des biens, les menaces et les vulnérabilités. Par exemple, la mesure de prévention qui ramène une vulnérabilité connexe de niveau Élevé au niveau Faible est évidemment plus efficace que celle

qui la ramène seulement au niveau Moyen. Certains autres facteurs, comme la sensibilité, la visibilité et l'acceptabilité d'une mesure de protection, sa propre vulnérabilité, toute interdépendance avec d'autres mesures de sécurité, la maturité du produit ou processus et sa conformité aux normes de sécurité nationales ou internationales, sont aussi des indicateurs utiles, quoique moins précis, de l'efficacité des mesures de protection.

3.3.2 Incidence sur les valeurs des biens

Plafonner les valeurs des biens, un mécanisme d'évitement, peut atténuer les risques dans certaines circonstances. La différence entre les valeurs des biens peut être mesurée avec précision en appliquant les critères de préjudice expliqués à la section 3 de l'annexe B, Phase d'identification et d'évaluation des biens. Ainsi, la limite de transaction de 1 000 $ est plus efficace que celle de 1 million de dollars, car elle ramène les valeurs des biens de niveau Moyen au niveau Faible.

3.3.3 Incidence sur les menaces

Certains mécanismes de dissuasion peuvent décourager les agents de menace délibérée, réduisant ainsi la probabilité qu'une situation de menace se produise. Le choix d'emplacements moins vulnérables à certains sinistres naturels peut avoir le même effet. Quelques mesures préventives, comme restreindre la possession des outils de crochetage des serrures, peuvent réduire les capacités des agents de menace et donc la gravité d'un incident. Dans chaque cas, le niveau de la menace peut être recalculé afin de tenir compte de l'incidence des mesures de protection recommandées. Les mesures qui réduisent davantage les niveaux de menace sont plus efficaces.

3.3.4 Incidence sur les vulnérabilités

Comme il est indiqué à la section 3.3 de l'annexe D, Évaluation de la vulnérabilité, la plupart des mesures de protection s'attaquent aux vulnérabilités plutôt qu'aux valeurs des biens et aux menaces afin d'atténuer les risques inacceptables. Par exemple, la plupart des mesures de prévention réduisent la probabilité de compromission au cas où une situation de menace se matérialiserait, tandis que les mécanismes de détection, d'intervention et de reprise visent à limiter ou à circonscrire les dommages et à modérer la gravité des résultats. Comme pour les valeurs des biens et menaces, les niveaux de vulnérabilité peuvent être révisés de manière à tenir compte de l'incidence des mesures de sécurité proposées : là encore, plus la différence est grande, plus la mesure de protection est efficace.

3.3.5 Acceptabilité

L'efficacité des mesures de protection dépend souvent de son acceptation par l'utilisateur et l'exploitant. À cet égard, la commodité et la facilité d'emploi sont importantes, de sorte que les mesures de sécurité simples et conviviales sont souvent préférables aux solutions plus performantes mais complexes. Par exemple, un mécanisme de contrôle d'accès basé sur de multiples mots de passe imprononçables risque de susciter un sentiment de frustration et de s'avérer contre-productif. D'autres facteurs touchant l'acceptabilité d'une contre-mesure éventuelle pourraient concerner la sécurité réelle ou imaginée de certains dispositifs biométriques, comme les lecteurs d'empreintes rétiniennes, et la résistance sociale ou culturelle aux fouilles indiscrètes ou à la surveillance. Trop souvent, le mécanisme de sécurité n'est pas aussi efficace qu'il devrait l'être en théorie parce que l'employé ou le client s'y oppose. Néanmoins, lorsqu'un leadership compatissant et une formation

solide permettent de surmonter cette résistance, des utilisateurs bien informés et hautement motivés peuvent accroître l'efficacité de nombreuses mesures de protection.

3.3.6 Visibilité

Les mesures de protection hautement visibles, comme les clôtures à mailles de chaîne ou les patrouilles, peuvent être plus efficaces mais avoir des effets secondaires négatifs. Une trop grande visibilité peut attirer une attention inopportune et accroître la probabilité de certaines menaces délibérées. Elle peut aussi permettre aux adversaires d'étudier la situation afin de déceler les vulnérabilités exploitables.

3.3.7 Vulnérabilité des mesures de protection

Comme tout autre bien, les mesures de protection peuvent avoir leurs propres vulnérabilités. La fiabilité, la robustesse, la complexité, les autres enjeux de maintenance et la facilité d'emploi (ou d'abus) sont autant de facteurs influant sur la susceptibilité d'une contre-mesure aux défaillances accidentelles ou aux dérobades délibérées. Chacun de ces facteurs doit être évalué par rapport aux valeurs des biens et aux menaces incluses dans la portée du projet d'EMR. Autrement dit, les mesures de protection que les agents de menace connus peuvent exploiter de manière à compromettre les biens identifiés dans l'énoncé de sensibilité sont probablement moins efficaces que celles qui ne présentent aucune vulnérabilité perceptible ou pertinente.

3.3.8 Interdépendance des mesures de protection

Certaines mesures de protection agissent indépendamment, mais la plupart doivent être appuyées par des dispositifs de sécurité complémentaires pour produire l'effet désiré. Par exemple, l'efficacité de la meilleure serrure à pêne dormant dépend de l'intégrité structurale de la porte et de son cadre, et elle est facilement compromise par des fenêtres adjacentes non protégées. Les répercussions négatives de l'interdépendance des mesures de protection reflètent le vieil adage selon lequel la solidité de la chaîne est celle de son maillon le plus faible. D'un point de vue positif, par contre, les mesures de sécurité étroitement intégrées qui s'appuient mutuellement sont souvent plus efficaces que la somme de leurs parties pour la défense en profondeur. Les deux facteurs doivent être pris en compte durant le processus de sélection des mesures de protection.

3.3.9 Intervention humaine

Parallèlement, les mesures de protection qui dépendent d'une intervention ou interprétation humaine sont souvent moins fiables que les mécanismes totalement automatisés, particulièrement si elles sont difficiles ou peu commodes à gérer. La nature humaine étant ce qu'elle est, seuls les individus les plus consciencieux resteront vigilants avec le temps et s'empresseront d'intervenir, particulièrement après plusieurs fausses alarmes. Les autres sont plus susceptibles d'ignorer ou de désactiver le détecteur ou l'alarme. Cela dit, les employés motivés qui ont reçu une formation appropriée peuvent accroître l'efficacité de certaines mesures de protection en faisant une interprétation intelligente des données conflictuelles et en répondant de façon mesurée à différents incidents. Les deux possibilités doivent être examinées durant l'évaluation de l'efficacité des mesures de protection.

3.3.10 Sensibilité

Comme d'autres biens, les mécanismes de sécurité peuvent être vulnérables à une divulgation non autorisée et doivent donc être classés comme classifiés ou protégés selon que les intérêts auxquels une compromission pourrait porter préjudice sont d'envergure nationale ou autre. Il s'agit généralement d'un facteur important dans le cas des dispositifs cryptographiques et du matériel de chiffrement connexe. Comme les mesures de protection classifiées et protégées exigent habituellement une protection supplémentaire pour préserver leur confidentialité, elles sont souvent moins souhaitables que les contre-mesures non classifiées.

3.3.11 Technologies éprouvées

Les produits de sécurité éprouvés ont tendance à être plus efficaces que les nouvelles technologies arrivées sur le marché. Dans la pratique, toutefois, la différence réelle peut être difficile à déterminer, sauf si la mesure de protection a fait l'objet d'une évaluation formelle quelconque. Quoi qu'il en soit, entre deux solutions comparables, le produit plus stable est généralement préférable.

3.3.12 Normes de sécurité

Divers organismes de normalisation, nationaux et internationaux, élaborent des pratiques et procédures communes pour la sélection, l'installation ou l'application et l'utilisation des produits et processus de sécurité. Dans certains cas, ils accréditent également des laboratoires pour la conduite de tests et d'évaluations formels.[3] Les normes peuvent présenter les lignes directrices générales en matière de sécurité, définir les pratiques exemplaires généralement reconnues, ou établir des méthodes formelles pour l'évaluation du matériel et des produits de sécurité. En règle générale, les mesures de protection conformes à l'une ou plusieurs des normes sont censées être plus efficaces. Sauf dans quelques exceptions notables, comme les *Critères communs pour l'évaluation des produits relatifs à la sécurité des technologies de l'information*,[4] la conformité aux normes approuvées donne peu d'indications sur l'efficacité relative des mesures de protection aux fins de l'analyse comparative des différentes options. Il reste que les mesures de sécurité fondées sur les normes reconnues sont généralement préférables aux autres options, à condition d'être pleinement mises en œuvre et configurées de façon à respecter toutes les dispositions de la norme pertinente.

3.4 Résumé

En résumé, le processus de sélection des mesures de protection comporte deux étapes successives.

---

[3] Certains de ces organismes de normalisation sont énumérés à l'**appendice F-1**, **Sources des données sur les mesures de protection**.

[4] Le Schéma lié aux Critères communs permet une évaluation explicite du niveau d'assurance associé aux dispositifs de sécurité d'un produit de sécurité des TI. Ce niveau d'assurance évalué peut se traduire directement par une évaluation relative de l'efficacité de la mesure de protection. Le CST offre actuellement un cours d'une journée, CST 755, Choisir les technologies de sécurité appropriées : Mise en correspondance de l'EMR aux Critères communs, qui explique le processus. De plus amples détails figurent à http://www.cse-cst.gc.ca/training/courses/755-f.html.

Il faut d'abord identifier les mesures de sécurité susceptibles de parer aux risques résiduels inacceptables. À cette fin, la liste des risques résiduels évalués établie durant la phase précédente du projet d'EMR peut être triée selon différents champs afin de confirmer les biens, menaces et vulnérabilités qui contribuent aux plus grands risques. De toute évidence, les mesures de protection doivent être choisies pour protéger ces biens et leurs valeurs, et atténuer les menaces et vulnérabilités connexes.

Il ne suffit pas de savoir quelles mesures de sécurité offrent le genre de protection requise sur le plan qualitatif pour atteindre des niveaux acceptables de risque résiduel. Il faut aussi déterminer le niveau de protection requis pour ramener tous les risques dans une fourchette acceptable. En conséquence, la deuxième phase du processus de sélection des mesures de protection comprend une évaluation de l'efficacité des mesures de protection, une mesure quantitative de leur incidence sur les valeurs des biens, les menaces et les vulnérabilités, tempérée par des considérations plus subjectives.

À la fin de ce processus, l'équipe d'EMR devrait avoir identifié au moins une mais, de préférence, plusieurs options pour parer à chaque risque inacceptable.

L'appendice F-3 contient une liste des critères de sélection des mesures de protection ainsi que des instructions détaillées expliquant comment appliquer ces critères.

4 Identification des coûts connexes

4.1 Principal objectif

Une fois qu'on aura identifié un ensemble de mesures de protection susceptibles de remédier aux risques résiduels inacceptables, l'équipe d'EMR devra déterminer les options qui offrent le meilleur rapport qualité-prix. Les coûts directs et indirects associés à chaque mesure de protection devraient être comptabilisés le plus exactement possible afin d'éclairer la prise des décisions et de justifier les recommandations finales au responsable de l'acceptation des risques.

4.2 Coûts directs

La plupart des coûts directs ou, à tout le moins, des estimations raisonnables sont disponibles auprès des gestionnaires de projet, des bureaux d'étude, des responsables de l'approvisionnement, des fournisseurs de produits et de nombreuses sources listées à l'appendice F-1. Les principaux facteurs à prendre en considération comprennent :

- **La conception et le développement.** Bien que la plupart des mesures de protection visant le matériel et les procédures de sécurité puissent être achetées directement, il pourrait être nécessaire, dans certains cas, d'en assurer la conception et le développement à l'interne ou par l'entremise d'un sous-traitant. C'est habituellement le cas pour les nouvelles installations, les rénovations importantes, les systèmes de TI complexes et les grands projets de l'État où les considérations en matière de sécurité représentent généralement entre 5 % et 10 % du budget total. Même les solutions recommandées pour

les petits projets d'EMR pourraient prévoir des coûts pour les travaux d'architecture et d'ingénierie liés aux études de faisabilité, à la conception et au développement.

- **L'acquisition.** Les coûts les plus visibles associés aux recommandations seront le prix d'achat ou les droits de permis pour le matériel, les logiciels ou les procédures de sécurité. Dans la plupart des cas, il est facile d'obtenir des estimations précises auprès du fournisseur original ou du revendeur.
- **L'intégration.** Des efforts sont presque toujours requis pour intégrer les mesures de protection recommandées aux installations, au matériel, aux logiciels ou aux procédures existantes. Les coûts connexes ressemblent beaucoup à ceux engagés pour les grands projets, les plus grandes dépenses étant généralement les salaires du personnel de conception, de développement et d'essai.
- **L'installation.** Les coûts d'installation peuvent être inclus dans les dépenses d'intégration, mais ils peuvent aussi être calculés séparément, particulièrement lorsque les mesures de protection recommandées doivent être déployées à l'échelle régionale et exigent donc un généreux budget de déplacement.
- **La documentation.** Le prix d'achat de nombreuses mesures de protection comprend un ensemble complet de documents tels qu'un guide de l'utilisateur, une notice d'installation et un manuel de l'opérateur. Cependant, il est parfois nécessaire de documenter la configuration réelle du nouveau matériel de sécurité et de préparer des procédures normales d'exploitation spécifiques au site. La mise à jour de cette documentation est une autre dépense permanente souvent négligée.
- **La formation.** Il est généralement nécessaire d'engager des coût de formation sur le nouveau matériel de sécurité et les procédures connexes pour s'assurer que le matériel est installé et qu'il fonctionne correctement. Là encore, il peut s'agir d'une dépense permanente étant donné la mobilité du personnel entre les postes et les organisations.
- **Les activités courantes.** Les coûts de fonctionnement pour les mesures de protection recommandées couvrent diverses dépenses, dont la rémunération et les avantages sociaux des gardiens de sécurité et autres membres du personnel, le matériel et les fournitures consommables, les permis renouvelables et autres droits, les mises à niveau périodiques, les vérifications et examens, ainsi que la mise à jour de la formation et de la documentation si ces postes ne sont pas comptabilisés séparément, comme il est indiqué plus haut.
- **La maintenance.** Les coûts de maintenance systématique peuvent être comptabilisés sous les charges de fonctionnement, mais des fonds distincts peuvent être mis de côté pour la réparation ou le remplacement du matériel défectueux selon l'évaluation du temps moyen entre défaillances.

4.3 Coûts ou avantages indirects

Dans la plupart des cas, les coûts ou avantages indirects associés aux mesures de protection potentielles sont beaucoup plus difficiles à prévoir avec précision parce que le plein effet de leur mise en œuvre pourrait ne pas être évident en l'absence d'expérience opérationnelle. Il faut néanmoins s'efforcer de projeter les coûts et avantages indirects suivants dans la mesure du possible :

- **Productivité réduite.** Certaines mesures de protection peuvent causer des retards ou des distractions et nuire à la productivité. Par exemple, les contrôles d'accès rigoureux et les vérifications ponctuelles risquent de ralentir la circulation des piétons et des véhicules à l'entrée des installations sécurisées. Les fonctions de vérification, manuelles et automatisées, entraînent des frais généraux pour le personnel et le matériel de TI et ont une incidence correspondante sur la capacité de production. En général, ces coûts sont des irritants relativement mineurs pleinement compensés par d'autres avantages, mais ils doivent être identifiés de façon explicite dans la mesure du possible afin d'assurer une évaluation équilibrée.
- **Efficacité accrue.** En théorie, la plupart des mesures de protection devraient avoir un effet positif sur l'efficience en ramenant la probabilité et la gravité des compromissions à des niveaux acceptables proportionnés aux besoins opérationnels établis. Les mesures de protection relatives à la disponibilité, comme la planification de la continuité des activités, offrent sans doute les meilleurs exemples parce que les coûts des interruptions et les avantages d'une reprise rapide peuvent être mesurés avec précision.

4.4 Rentabilité

4.4.1 Approche de base

Après avoir identifié un ensemble de mesures de protection possibles en se fondant sur des critères de sélection explicites (section 3.2) et déterminé le coût total de la propriété pour chaque option (sections 4.2 et 4.3), l'équipe d'EMR pourrait avoir à faire des choix difficiles entre les options viables. Il faudra donc évaluer la rentabilité réelle de chaque proposition afin de fournir une justification objective à l'appui des recommandations finales. À cet égard, les deux principaux facteurs à prendre en considération sont le coût annuel amorti des mesures de sécurité recommandées et leur incidence globale sur le risque résiduel, le coût et l'efficacité, mais d'autres questions pourraient se poser dans la pratique.

4.4.2 Coût annuel amorti

Le coût total de la possession est important en termes absolus, particulièrement parce qu'une grande partie des dépenses, comme les frais d'acquisition et d'installation, sont engagées au début du processus. Ce chiffre doit toutefois être tempéré par la durée utile prévue des mesures de protection proposées. Certaines, comme les dispositifs de sécurité physique intégrés à la structure d'un immeuble, durent très longtemps tandis que d'autres, comme les logiciels de sécurité, ont une vie utile beaucoup plus courte. En termes pratiques, une contre-mesure coûteuse mais durable peut offrir un meilleur rapport qualité-prix qu'une option plus économique qu'il faudra vite remplacer. Ainsi, le coût annuel amorti, obtenu en divisant le coût total de possession par la durée utile prévue, selon la formule illustrée à la figure F-2, est le premier facteur analytique justifiant les recommandations finales.

$$\frac{\text{Coût total de possession (\$)}}{\text{Durée utile prévue (années)}} = \text{Coût annuel amorti (\$/année)}$$

Figure F-2 : Calcul du coût annuel amorti

4.4.3 Réduction totale du risque

Comme il est indiqué à la section 3.3.1, les mesures de protection atténuent le risque en réduisant une ou plusieurs de trois variables : les valeurs des biens, les menaces et les vulnérabilités. En outre, certaines mesures de sécurité, comme les contrôles d'accès physiques, protègent de nombreux biens et valeurs de biens contre différentes menaces, parant ainsi à un large éventail de risques. D'autres, comme les déchiqueteuses à papier, visent une seule valeur (la confidentialité) pour un nombre limité de biens (documents classifiés et protégés) afin de s'attaquer à une gamme étroite de menaces (activités de menace causant une divulgation non autorisée). Bien que les deux types de mesures puissent être nécessaires dans une situation donnée, les mesures de sécurité qui ramènent plus de risques à un niveau acceptable offrent généralement un meilleur rapport qualité-prix. La réduction totale du risque, deuxième critère servant à déterminer la rentabilité relative de différentes options, peut être calculée comme suit :

- dans la liste des risques résiduels évalués (appendice E-2), choisir toutes les combinaisons de risques inacceptables (valeur des biens, menace et vulnérabilité) qui sont modérées par la mesure de protection proposée;
- recalculer le risque résiduel pour chacune des entrées, en se fondant sur la plus faible valeur, menace ou vulnérabilité obtenue grâce à la mesure de protection proposée;
- déterminer le nombre de niveaux entre les risques résiduels évalués et ceux projetés pour chaque combinaison touchée par la mesure de protection proposée;
- calculer la réduction totale du risque en faisant le total des changements dans les niveaux de risque.

4.4.4 Mesures de protection recommandées

Idéalement, les recommandations du rapport final d'EMR, une fois approuvées et mises en œuvre, devraient ramener les risques résiduels inacceptables à des niveaux acceptables au moindre coût ou au coût le plus raisonnable. Lorsque plus d'une option est identifiée durant le processus de sélection des mesures de protection décrit à la section 3 ci-dessus, il faut classer les options par ordre de rentabilité décroissante, la rentabilité relative étant obtenue en divisant le coût annuel amorti par la réduction totale du risque, selon la formule illustrée à la figure F-3. Il sera alors possible de déterminer et de recommander l'ensemble le plus rentable de mesures de protection susceptibles de remédier aux risques résiduels inacceptables. Ces recommandations doivent être résumées sous forme de tableau à l'appendice F-5.

$$\frac{\text{Coût annuel amorti (\$/année)}}{\text{Réduction totale du risque (niveaux)}} = \text{Rentabilité (\$/année/niveau)}$$

Figure F-3 : Calcul de la rentabilité des mesures de protection

4.4.5 Considérations pratiques

Dans quelques cas, le calcul de la rentabilité peut être sans objet parce qu'il existe une seule mesure de protection pouvant atténuer un risque résiduel particulier, ou parce que la solution est dictée par des normes gouvernementales approuvées. Il peut aussi arriver que la solution la plus efficace soit beaucoup trop coûteuse. Si les options abordables ne permettent pas d'atteindre les niveaux de risque visés, il peut être nécessaire de recommander un examen des exigences originales, le rejet de la proposition ou l'annulation du projet, comme il est expliqué à la section 2.4.3. Plus souvent qu'autrement, la véritable difficulté consistera à choisir entre plusieurs options, qui offrent toutes une réduction acceptable des risques mais de différentes façons et à différents prix. Quoi qu'il en soit, le calcul de la rentabilité des différentes mesures de protection, qui est présenté plus haut et explicité à l'appendice F-4, constitue un point de départ objectif pour les recommandations finales sur les moyens de parer aux risques résiduels inacceptables ou d'identifier les risques impossibles à éliminer.

5 Évaluation des risques résiduels projetés

Pour illustrer l'incidence de ces recommandations dans le rapport final d'EMR, les risques inacceptables de la liste des risques résiduels évalués à l'appendice E-2 devraient être inscrits dans les colonnes appropriées sous les mesures de protection compensatoires du tableau des recommandations. Les risques résiduels qui restent après l'approbation et la mise en œuvre des propositions devraient ensuite être calculés et inscrits au tableau, comme l'expliquent les instructions détaillées de l'appendice F-5.

6 Rapport final d'EMR

6.1 Format du rapport d'EMR

À cette étape, les résultats de chacune des phases précédentes du projet d'EMR peuvent être combinés et résumés dans une analyse narrative logique étayée par des documents qui expliquent et justifient les recommandations finales. Il est toutefois essentiel de faire preuve de concision afin de promouvoir et de faciliter l'examen par la direction. Chaque section doit donc mettre l'accent sur les points les plus importants, les détails pouvant être exposés dans les tableaux récapitulatifs et les annexes. Le format du rapport d'EMR varie selon l'objet de l'évaluation, mais il contient généralement les rubriques suivantes :

- **Résumé.** À moins d'être très courts, tous les rapports d'EMR doivent commencer par un résumé d'une ou deux pages qui décrit l'objet et le sujet de l'évaluation, les risques résiduels évalués inacceptables, les principales recommandations, le coût total de toutes

les propositions et les risques résiduels projetés une fois les recommandations approuvées et mises en œuvre.

- **Contexte.** Comme il est indiqué à la section 1 de l'appendice A-6, Exemple de plan de travail de l'EMR, identifier l'organisation et situer l'évaluation dans un contexte ministériel. Selon l'objectif de l'EMR, cela peut inclure :
    - une brève description du secteur d'activité et de son environnement opérationnel;
    - les niveaux de prestation de services ou les obligations pertinents à l'évaluation;
    - la justification de l'acquisition ou de la mise à niveau d'une installation ou d'un système de TI;
    - la nature des préoccupations en matière de sécurité.
- **But.** Comme il est expliqué à la section 2 de l'appendice A-6, Exemple de plan de travail de l'EMR, indiquer le but de l'évaluation en une seule phrase, comme dans les exemples suivants :
    - « Le but de cette EMR est d'évaluer les risques associés aux mises à niveau prévues pour [nom de l'installation] et de recommander des mesures de protection appropriées. »
    - « Le but de cette EMR est d'évaluer les risques associés à [nom du nouveau système de TI] et de recommander des mesures de protection appropriées à l'appui de la certification et l'accréditation des systèmes. »
    - « Le but de cette EMR est d'évaluer le besoin de mesures de protection au-delà des exigences de base en matière de sécurité de [nom de l'installation ou du système de TI]. »
- **Mandat.** Passer brièvement en revue les pouvoirs de l'équipe d'EMR établie conformément à la section 3 de l'annexe A, Phase de préparation. Joindre en annexe une copie de toute instruction écrite et du plan de travail de l'EMR décrit à l'appendice A-6.
- **Portée.** Comme il est indiqué à la section 4 de l'annexe A, Phase de préparation, indiquer le sujet de l'évaluation et donner une description générale de l'installation ou du système de TI en cours d'évaluation. Les cartes, graphiques, plans d'étage et schémas de système peuvent être particulièrement utiles pour représenter les limites d'un projet d'EMR. Noter toute EMR connexe et expliquer comment elle se rapporte au projet en cours. Vous pouvez joindre en annexe les listes des éléments qui sont inclus ou qui ne sont pas inclus dans la portée de l'évaluation.
- **Identification et évaluation des biens.** Une fois que tous les biens, corporels ou incorporels, les employés et les services inclus dans la portée de l'évaluation ont été identifiés et que des valeurs basées sur les critères de préjudice expliqués à l'annexe B leur ont été attribuées, les conclusions doivent être annexées au rapport d'EMR sous forme de tableau d'évaluation des biens ou d'énoncé de sensibilité, lesquels sont illustrés à l'appendice B-5. Le corps du texte doit contenir un bref résumé axé sur les biens et valeurs les plus importants et leur relation avec les secteurs d'activités ou objectifs opérationnels de l'organisation.
- **Évaluation des menaces.** Une liste complète des menaces et niveaux de menace doit être annexée au rapport d'EMR sous la forme indiquée à l'appendice C-4, Tableau d'évaluation des risques. Seules les menaces plus graves touchant les biens de plus grande valeur, généralement ceux des catégories Élevé et Très élevé, doivent être examinées brièvement dans le corps du rapport d'EMR.

- **Évaluation des vulnérabilités.** Comme l'énoncé de sensibilité et l'évaluation des risques, l'évaluation des vulnérabilités doit comprendre une brève explication des principales lacunes de sécurité dans le rapport principal ainsi qu'une annexe sous la forme de l'appendice D-4, Tableau d'évaluation des vulnérabilités, énumérant tous les problèmes.
- **Évaluation des risques.** L'Évaluation des risques peut être la partie la plus longue et la plus complexe de nombreux rapports d'EMR parce que chaque risque résiduel inacceptable doit être expliqué en termes utiles au responsable de l'acceptation des risques. Bien sûr, les résultats doivent être comprimés et résumés le plus possible et les détails, reportés à une annexe telle que l'appendice E-2, Liste des risques résiduels évalués, mais le texte doit préciser les rapports qui existent entre les valeurs des biens, les menaces et les vulnérabilités, et leur incidence sur les risques résiduels. Cela peut constituer un défi lorsque les pires risques découlent de menaces accrues touchant des biens de valeur plus faible, car de nombreux gestionnaires ont tendance à mettre l'accent sur les biens les plus importants plutôt que sur les risques auxquels ils sont exposés.
- **Recommandations.** Du point de vue de la direction, les recommandations représentent la partie la plus importante du rapport d'EMR. Les coûts associés à chaque recommandation et le risque résiduel projeté doivent être expliqués avec soin en termes non techniques afin de solliciter l'appui et l'approbation de la direction. Comme dans les sections précédentes, la plupart des détails de l'analyse des coûts et de l'efficacité des mesures de protection doivent être exposés dans une annexe basée sur l'appendice F-5, Tableau des recommandations.
- **Pièces jointes.** Afin de simplifier le corps du texte, l'information à l'appui du rapport d'EMR doit être présentée dans une série de pièces jointes ou d'annexes comprenant :
    - le mandat d'EMR;
    - le plan de travail de l'EMR;
    - la portée de l'évaluation;
    - les rapports d'EMR connexes;
    - le tableau d'évaluation des biens ou l'énoncé de sensibilité;
    - le tableau d'évaluation des menaces;
    - le tableau d'évaluation des vulnérabilités;
    - le tableau des risques résiduels;
    - le tableau des recommandations;
    - la liste des documents de référence, c'est-à-dire tous les manuels, schémas, rapports d'incident et autres documents consultés durant le projet d'EMR qui constituent le dossier à l'appui du rapport d'EMR.

L'appendice F-6 renferme un Plan du rapport sur l'EMR avec notes explicatives et renvois aux sections pertinentes de la *Méthodologie harmonisée d'EMR* sous forme d'aide-mémoire ou de liste de contrôle pour les analystes de la sécurité, tandis que l'appendice F-7 présente un modèle de rapport d'EMR dans son ensemble.

6.2 Rapport d'EMR et dossier d'EMR

Comme il est noté tout au long de la *Méthodologie harmonisée d'EMR*, depuis la phase de préparation jusqu'à la phase finale des recommandations, différentes sources d'information doivent être consultées afin d'identifier les biens inclus dans la portée de l'évaluation, d'en déterminer les valeurs, de saisir les données pertinentes sur les menaces, de déceler les vulnérabilités associées et de choisir les mesures de protection rentables.[5] En fait, pour tous les projets d'EMR sauf les plus simples, la liste de documents de référence peut être très longue. Bien qu'essentielles pour appuyer le processus analytique, ces références ne doivent généralement pas accompagner le rapport final sur l'EMR. Elles doivent toutefois être citées dans une annexe et versées au dossier pour examen futur dans le cadre du dossier permanent de l'EMR.

5 Certaines de ces sources de données sont énumérées à :

- la section 8 de **l'appendice A-6**, **Exemple de plan de travail de l'EMR**;
- **l'appendice B-1**, **Sources des données sur les biens**;
- **l'appendice C-1**, **Sources des données sur les menaces**;
- **l'appendice D-1**, **Sources des données sur les vulnérabilités**; et
- **l'appendice F-1, Sources des données sur les mesures de protection.**

Page intentionnellement laissée en blanc

Appendice F-1 - Sources de données sur les mesures de protection

Ressources ministérielles	
Source de données/Documentation	**Classe/Groupe de mesures de protection**
Gestionnaires de programme • Plans d'activités • Procédures normales d'exploitation	• Programme de sécurité o Rôles et responsabilités o Ressources humaines o Ressources financières o Procédures de sécurité • Partage de l'information et des biens o Information • Marchés • Identification des biens • Sanctions
Gestionnaires du matériel/des biens • Répertoires des biens • Procédures normales d'exploitation	• Marchés • Sécurité matérielle o Entreposage sécurisé
Gestionnaires des installations • Plans d'étage/schémas des immeubles • Instructions pour le personnel de garde • Procédures de contrôle d'accès • Plans d'intervention d'urgence • Procédures de réaction aux incidents	• Partage de l'information et des biens o Installations • Protection des employés o Réponse de la direction/Mesures de protection • Sécurité matérielle o Sécurité du périmètre o Contrôles d'accès o Gestion des installations
Ressources humaines • Procédures de réaction aux incidents	• Protection des employés
Finances • Procédures normales d'exploitation	• Restrictions d'accès o Disponibilité/intégrité/séparation des tâches
Dirigeant principal de l'information • Accords sur les niveaux de service • Modalités de partage des biens • Normes/Directives en matière de sécurité des TI	• Partage de l'information et des biens o Infrastructure des TI • Sécurité des TI o Contrôles de gestion o (Quelques) mesures de protection techniques o Mesures de protection opérationnelles

Ressources ministérielles	
Source de données/Documentation	**Classe/Groupe de mesures de protection**
Administrateur (de la sécurité) des systèmes • Schémas des systèmes • Procédures normales d'exploitation • Test de sécurité/rapports d'évaluation • Registres/rapports des incidents	• Sécurité des TI o (Quelques) contrôles de gestion o Mesures de protection techniques o Mesures de protection opérationnelles
Agent de sécurité du ministère • Directives ministérielles sur la sécurité • Procédures normales d'exploitation • Rapports d'inspection sur la sécurité • Rapports d'enquête	• Programme de sécurité • Marchés • Sensibilisation/formation en matière de sécurité • Identification des biens • Gestion des risques liés à la sécurité • Filtrage de sécurité • Protection des employés • Sécurité matérielle • Sécurité en situations d'urgence • Enquête sur les incidents • Sanctions
Coordonnateur de la sécurité des TI • Examens/évaluations des produits • Rapports d'incidents	• Enquêtes/incidents concernant la sécurité des TI
Coordonnateur de la PCA • Plans de continuité des activités • Exercice sur les PCA/résultats des tests	• Planification de la continuité des activités
Vérification interne/examen • Vérifications/examens de la sécurité	• Programme de sécurité (tout contrôle de gestion assujetti à une vérification ou à un examen)
Santé et sécurité au travail • Procédures normales d'exploitation • Rapports d'enquête/d'incident	• Protection des employés o Gestion des incidents

Ressources externes : Ministères responsables de la sécurité	
Source de données/Documentation	**Types de mesure de protection**
Centre de la sécurité des télécommunications http://www.cse-cst.gc.ca/publications/publications-f.html • Guides et directives sur la sécurité des TI • Alertes et bulletins de sécurité des TI http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-f.html • Rapports de certification de produits évalués	• Sécurité des TI
Sécurité publique et Protection civile Canada http://www.psepc-sppcc.gc.ca/prg/em/index-fr.asp • Publications/avis analytiques	• Protection des infrastructures essentielles • Cybersécurité • Atténuation des catastrophes • Protection civile
Gendarmerie royale du Canada http://www.rcmp.ca/tsb/pubs/index_f.htm • Guides/rapports sur la sécurité	• Sécurité matérielle • Sécurité des TI
Travaux publics et Services gouvernementaux Canada http://www.ciisd.gc.ca/text/ISM/toc-f.asp • **Manuel de la sécurité industrielle**	• Sécurité des marchés

Ressources externes : Organisations des normes gouvernementales	
Source de données	**Types de mesure de protection**
Conseil national de recherches http://www.nationalcodes.ca/ncd_home_f.shtml • Code national du bâtiment du Canada • Code national de prévention des incendies du Canada	• Sécurité et protection personnelles
Conseil canadien des normes http://www.scc.ca/fr/index.shtml • Plusieurs normes sur la sûreté et la sécurité	• Types variés

Ressources externes : Autres organismes de normes	
Source de données	**Types de mesure de protection**
American National Standards Institute http://www.ansi.org/	• Normes sur la sécurité des TI
Association canadienne de normalisation http://www.csa.ca/about/Default.asp?language=french	• Normes sur la santé et la sécurité

Organisation internationale de normalisation http://www.iso.org/iso/fr/ISOOnline.frontpage	• Plusieurs normes sur la sûreté et la sécurité • Normes sur la sécurité des TI
Union internationale des télécommunications http://www.itu.int/net/home/index-fr.aspx	• Normes sur les TI et sur la sécurité des TI
National Institute of Standards and Technology http://www.nist.gov/	• Normes sur les TI et sur la sécurité des TI
Organisation de coopération et de développement économiques http://www.oecd.org/home/0,2605,fr_2649_201185_1_1_1_1_1,00.html	• Normes sur la sécurité des TI et sur la protection des renseignements personnels

Ressources externes : Autres organismes du secteur privé	
Source de données	**Types de mesure de protection**
Centre de coordination CERT (en anglais) http://www.cert.org/nav/index_green.html	• Vulnérabilités techniques
Critères communs (en anglais) http://www.commoncriteriaportal.org/public/consumer	• Lignes directrices sur la sécurité des TI
Ressources relatives à la sécurité informatique et de l'information de l'Institut SANS (en anglais) http://www.sans.org/resources/resources.php	• Mesures de protection relatives à la sécurité des TI
Fournisseurs de produits	• Fonctions de sécurité techniques

Nota :

1. Cette liste n'est pas exhaustive. D'autres éléments s'y ajouteront occasionnellement. Toute suggestion de documents de référence ou de contacts à ajouter peut être présentée aux bureaux mentionnés dans l'Avant-propos.
2. L'inclusion d'un site Web ne doit pas être interprétée comme une approbation. De la même manière, l'exclusion de sources qui pourraient se révéler utiles ne signifie pas qu'elles sont rejetées. La liste vise simplement à illustrer la richesse des renseignements facilement accessibles aux spécialistes de la sécurité et aux gestionnaires de risques.

Appendice F-2 – Liste des mesures de protection

Classe de mesures Groupe de mesures Mesure de protection	Incidence			Biens protégés	Valeurs protégées			Menaces atténuées	Référence(s)
	B_{Val}	M	V		C	D	I		
Programme de sécurité									PGS 10.1
Rôles et responsabilités									
Haute direction	√		√	Tous	√	√	√	Toutes	GSTI 9.2
Gestionnaires de programme	√		√	Tous	√	√	√	Toutes	GSTI 9.6
Gestionnaires de projet	√		√	Tous	√	√	√	Toutes	GSTI 9.6 et 9.10
Dirigeant principal de l'information	√		√	Tous	√	√	√	Toutes	GSTI 9.4
Employés			√	Tous	√	√	√	Toutes	GSTI 9.8
Agent de sécurité du ministère			√	Tous	√	√	√	Toutes	PGS 10.1 et GSTI 9.3
Coordonnateur de la sécurité des TI			√	I, T, S	√	√	√	Toutes	GSTI 9.1
Gardien COMSEC			√	I	√		√	E, C, A	GSTI 9.9
Coordonnateur de la PCA			√	Tous		√		S, T, C, A, N	GSTI 9.5
Ressources humaines									
Effectif			√	Tous	√	√	√	Toutes	
Niveaux de classification			√	Tous	√	√	√	Toutes	
Ressources financières									
Activités ministérielles			√	Tous	√	√	√	Toutes	
Projets			√	Tous	√	√	√	Toutes	GSTI 9.2
Politique et procédures de sécurité									
Partage d'information/de biens	√		√	I, T, INS, S	√	√	√	E, S, C, A	PGS 10.2
Marchés	√		√	I, S	√	√	√	E, S, C	PGS 10.4
Formation/sensibilisation en matière de sécurité			√	Tous	√	√	√	Toutes	PGS 10.5
Identification des biens	√		√	I	√	√	√	Toutes	PGS 10.6
Gestion des risques liés à la sécurité			√	Tous	√	√	√	Toutes	PGS 10.7
Restrictions d'accès			√	Tous	√	√	√	E, S, s, T, C, A	PGS 10.8
Filtrage de sécurité			√	Tous	√	√	√	E, S, s, T, C, A	PGS 10.9
Protection des employés			√	P		√		S, s, T,C, A, N	PGS 10.10
Sécurité matérielle			√	Tous	√	√	√	Toutes	PGS 10.11
Sécurité des TI			√	I, T, S	√	√	√	Toutes	PGS 10.12, GSTI 10, MG-01 Appendice C et MG-09 5
Sécurité en situations d'urgence			√	Tous	√	√	√	S, T, A, N	PGS 10.13
Planification de la continuité des activités			√	Tous		√		S, T, C, A, N	PGS 10.14
Vérification du programme de sécurité			√	Tous	√	√	√	Toutes	PGS 11
Enquête sur les incidents			√	Tous	√	√	√	Toutes	PGS 10.15
Sanctions		√	√	Tous	√	√	√	E, S, s, T, C, A	PGS 10.16
Partage d'information/de biens									PGS 10.2
Information									
Modalités	√		√	I, S	√	√	√	E, S, C, A	
Installations									G1-027

Classe de mesures Groupe de mesures Mesure de protection	Incidence			Biens protégés	Valeurs protégées			Menaces atténuées	Référence(s)
	B_{Val}	M	V		C	D	I		
Modalités	√		√	INS, S	√	√	√	E, S, C, A	
Infrastructure des TI									GSTI 12.10
Modalités	√		√	I, T, S	√	√	√	E, S, C, A	
Sécurité à l'extérieur du Canada									PGS 10.3
Normes spéciales									
EMR par établissement			√	Tous	√	√	√	Toutes	
Restrictions sur les voyages									
Selon l'établissement		√	√	P, I	√	√		E, T, C, N	MAECI
Marchés									PGS 10.4, SGM et MSI
Rôles et responsabilités									SGM 4-6
Autorité technique/autorité de projet			√	I	√			E, S, C	
LVERS	√		√	I	√			E, C	SGM 7
Attestation de sécurité des installations									SGM 8
Personnel responsable		√	√	I	√			E, C	
Protection des documents			√	I	√			E, C	
Marchés internationaux			√	I	√			E, S, C	SGM 10
Formation/sensibilisation en matière de sécurité									PGS 10.5, GSTI 12.12-12.13, MG-01 Appendice F, MG-09 13 et G1-030
Rôles et responsabilités									FSA 3
Agent de formation et de sensibilisation	√	√	√	Tous	√	√	√	E, S, s, T, C, A	
Formation en matière de sécurité									FSA 4.1
Spécialistes de la sécurité	√	√	√	Tous	√	√	√	E, S, s, T, C, A	
Sensibilisation à la sécurité									FSA 4.2
Breffages initiaux	√	√	√	Tous	√	√	√	E, S, s, T, C, A	FSA 4.3
Mises à jour régulières	√	√	√	Tous	√	√	√	E, S, s, T, C, A	FSA 8
Identification des biens									PGS 10.6 et IB
Confidentialité									IB 6.5
Cote de sécurité : Classifié	√		√	I	√			E, C	
Marquage : Classifié			√	I	√			E, C	IB 7.1 et MG-09 14.5
Cote de sécurité : Protégé	√		√	I	√			E, C	
Marquage : Protégé			√	I	√			E, C	IB 7.1 et MG-09 14.5
Disponibilité									IB 6.6
Cote de sécurité	√		√	Tous		√		S, T, C, A, N	
Marquage			√	Tous		√		S, T, C, A, N	
Intégrité									IB 6.7
Cote de sécurité	√		√	I			√	S, s, C, A	
Marquage			√	I			√	S, s, C, A	
Gestion des risques liés à la sécurité									PGS 10.7 et SRM
EMR									SRM 6 et MG-09 7
Filtrage initial	√		√	Tous	√	√	√	Toutes	
Surveillance continue	√		√	Tous	√	√	√	Toutes	
Restrictions d'accès									PGS 10.8
Biens classifiés/protégés									

Classe de mesures Groupe de mesures Mesure de protection	Incidence			Biens protégés	Valeurs protégées			Menaces atténuées	Référence(s)
	B_{Val}	M	V		C	D	I		
Besoin de connaître		√	√	I	√			E, C	
Filtrage de sécurité		√	√	Tous	√	√	√	E, S, s, T, C, A	
Disponibilité/Intégrité									
Division des tâches	√	√	√	Tous	√	√	√	S, s, T, C, A	
Filtrage de sécurité									PGS 10.9 et FS
Cote de fiabilité									FS 7
Établissement des exigences			√	Tous	√	√	√	E, S, s, T, C, A	
Filtrage initial		√	√	Tous	√	√	√	E, S, s, T, C, A	
Évaluation des résultats		√	√	Tous	√	√	√	E, S, s, T, C, A	
Mises à jour régulières		√	√	Tous	√	√	√	E, S, s, T, C, A	
Examen pour un motif déterminé		√	√	Tous	√	√	√	E, S, s, T, C, A	
Révocation		√	√	Tous	√	√	√	E, S, s, T, C, A	
Procédures de diffusion		√	√	Tous	√	√	√	E, S, s, T, C, A	
Cote de sécurité									FS 9-10
Établissement des exigences	√		√	I	√			E, C	
Filtrage initial		√	√	I	√			E, C	
Évaluation des résultats		√	√	I	√			E, C	
Mises à jour régulières		√	√	I	√			E, C	
Examen pour un motif déterminé		√	√	I	√			E, C	
Révocation/déclassement		√	√	I	√			E, C	
Procédures de diffusion		√	√	I	√			E, C	
Autorisation d'accès au site									FS 10.2
Établissement des exigences	√		√	I	√			E, C	
Filtrage initial		√	√	I	√			E, C	
Évaluation des résultats		√	√	I	√			E, C	
Mises à jour régulières		√	√	I	√			E, C	
Examen pour un motif déterminé		√	√	I	√			E, C	
Révocation		√	√	I	√			E, C	
Procédures de diffusion		√	√	I	√			E, C	
Protection des employés									PGS 10.10, PSST
Identification des employés à risque									
EMR			√	P		√		S, s, T, C, A, N	
Réponse de la direction									
Mesures de protection			√	P		√		S, s, T, C, A, N	
Mécanismes de soutien			√	P		√		S, s, T, C, A, N	
Formation et counselling			√	P		√		S, s, T, C, A, N	
Gestion des incidents									
Rapports d'incident			√	P		√		S, s, T, C, A, N	
Enquête sur les incidents			√	P		√		S, s, T, C, A, N	
Mesure corrective			√	P		√		S, s, T, C, A, N	
Sécurité matérielle									PGS 10.11 et SM
Facteurs de planification									G1-005
Codes du bâtiment			√	Tous	√	√	√	Toutes	G1-010
Zones de sécurité			√	Tous	√	√	√	E, S, s, T, C	SM, 6.2 et G1-026
Sélection de sites									SM 7
Servitudes		√	√	Tous		√		E, S, s, T, C	
Voies d'urgence			√	Tous		√		Toutes	

Classe de mesures Groupe de mesures Mesure de protection	Incidence			Biens protégés	Valeurs protégées			Menaces atténuées	Référence(s)
	B_{Val}	M	V		C	D	I		
Emplacement/topographie de l'immeuble		√	√	Tous		√		Toutes	
Services d'urgence			√	Tous		√		Toutes	
Occupants adjacents		√	√	Tous	√	√	√	E, S, C	
Sécurité du périmètre									SM 7.3
Contrôle du périmètre du site		√	√	Tous	√	√	√	E, S, s, T, C	
Éclairage du site		√	√	Tous	√	√	√	E, S, s, T, C, A	G1-002
Signalisation extérieure		√	√	Tous	√	√	√	E, S, s, T, C, A	
Aménagement paysager		√	√	Tous	√	√	√	E, S, s, T, C, A	
Stationnement		√	√	Tous	√	√	√	E, S, s, T, C, A	
Sécurité à l'entrée									SM 7.4
Entrées pour piétons/halls d'entrée			√	Tous	√	√	√	E, S, s, T, C	G1-017 et G1-018
Accès aux services publics			√	Tous	√	√	√	E, S, s, T, C	
Aires de réception/d'expédition			√	Tous	√	√	√	E, S, s, T, C	G1-015
Planification de la sécurité à l'intérieur			√						SM 7.5
Voies de circulation			√	P, INS		√		S, s, T, C, A	
Halls des ascenseurs			√	P		√		S, s, T, C	
Garderies			√	P		√		S, T, C, A	
Salles de réunion/conférence			√	P, I	√	√		E, S, s, T, C	
Escaliers/ascenseurs			√	P		√		S, s, T, C	
Toilettes			√	P		√		S, s, T, C	
Aires d'agrément			√	P		√		S, s, T, C	
Salles du courrier			√	P, I, INS	√	√		E, S, s, T, C	
Télécommunications/câblage			√	I	√	√	√	E, S, T, C, A	
Aires de CVC			√	F		√		S, s, T, C, A	
Salles des serveurs			√	I, T, S	√	√	√	E, S, s, T, C, A	G1-031
Contrôles d'accès									SM 7.6 et G1-025
Cartes d'identité			√	Tous	√	√	√	E, S, s, T, C	G1-005
Contrôles d'accès électroniques			√	Tous	√	√	√	E, S, s, T, C	
Dispositifs électroniques de détection des intrusions		√	√	Tous	√	√	√	E, S, s, T, C	
Équipement vidéo en circuit fermé		√	√	Tous	√	√	√	E, S, s, T, C, A	
Centre de contrôle de la sécurité			√	Tous	√	√	√	Toutes	G1-013
Locaux de réunion sécurisés			√	I	√			E, C	G1-004
Chambres fortes			√	I	√	√	√	E, S, s, T, C	G1-029
Gardes de sécurité		√	√	Tous	√	√	√	Toutes	G1-008
Gestion des installations									SM 7.7 et G1-027
Contrats de location	√		√	Tous	√	√	√	E, S, s, T, C, A	
Services d'entretien			√	Tous	√	√	√	E, S, s, T, C, A	
Services de nettoyage			√	Tous	√	√	√	E, S, s, T, C, A	
Signalisation intérieure		√		Tous	√	√	√	E, S, s, T, C, A	
Dispositif de verrouillage/contrôle des clés			√	Tous	√	√	√	E, S, s, T, C	G1-007 et G1-016
Travaux de rénovation			√	Tous	√	√	√	Toutes	
Comité de sécurité des installations	√		√	Tous	√	√	√	Toutes	
Entreposage sécurisé									SM 8

Classe de mesures Groupe de mesures Mesure de protection	Incidence			Biens protégés	Valeurs protégées			Menaces atténuées	Référence(s)
	B_{Val}	M	V		C	D	I		
Conteneurs de sécurité			√	I	√	√	√	E, C	G1-001
Clés/combinaisons			√	I	√	√	√	E, S, T, C	G1-007 et G1-016
Entretien des conteneurs			√	I	√	√	√	E, S, T, C	
Élimination des conteneurs			√	I	√			E, C	
Salles protégées/chambres fortes			√	I	√	√	√	E, C	G1-019 et G1-029
Transport/Transmission									SM 9 et G1-009
Transport	√		√	I	√		√	E, C	
Transmission	√		√	I	√		√	E, C	
Destruction									SM 10
Entreposage en attendant l'élimination			√	I	√			E, C, A	
Équipement de destruction : papier			√	I	√			E, C, A	
Équipement de destruction : soutien des TI			√	I	√			E, C, A	GSTI 16.2, DSX-G, G2-003 et ITSG-06
Marquage de l'équipement			√	I	√			E, C, A	
Entretien de l'équipement			√	I	√			E, C	
Services contractuels			√	I	√			E, C	
Destruction d'urgence			√	I	√			E, C	
Sécurité des TI									PGS 10.12 et GSTI
Contrôles de gestion									
Cycle de développement de système	√		√	I, T, S	√	√	√	Toutes	GSTI 12.1, MG-02, MG-09 8 et ITSA-09
Ressources destinées aux projets de sécurité des TI			√	I, T, S	√	√	√	Toutes	GSTI 11
Certification et accréditation	√	√	√	I, T, S	√	√	√	Toutes	GSTI 12.2.3 et MG-04
Marchés			√	I, T, S	√	√	√	E, S, C	GSTI 12.7
Impartition			√	I, T, S	√	√	√	E, S, C	
Sécurité matérielle et du personnel									G2-002
Sécurité matérielle			√	I, T, S	√	√	√	Toutes	G1-031 et GSTI 16.1
Sécurité du personnel		√	√	I, T, S	√	√	√	E, S, s, T, C, A	GSTI 16.3
Mesures de protection techniques									
Produits évalués			√	I, T, S	√	√	√	Toutes	GSTI 16.4.1
Identification et authentification			√	I, T, S	√	√	√	E, S, s, T, C, A	GSTI 16.4.2, MG-09 16 et R2-001
Autorisation et contrôle de l'accès			√	I, T, S	√	√	√	E, S, s, T, C, A	GSTI 16.4.3 et MG-09 17
Chiffrement			√	I	√		√	E, C	GSTI 16.4.4, ITSD-01 Annexe C, ITSB-013, ITSG-10, ITSG-13 et MG-09 19
Infrastructure à clé publique (ICP)			√	I, S	√	√	√	E, C	GSTI 16.4.5
Défense du périmètre			√	I, T, S	√	√	√	E, S, s, T, C	GSTI 16.4.6, ITSD-02, MG-01 &
Informatique mobile/télétravail	√		√	I, T, S	√	√	√	E, S, s, T, C, A	GSTI 16.4.7 et ITSPSR-14

Classe de mesures Groupe de mesures Mesure de protection	Incidence			Biens protégés	Valeurs protégées			Menaces atténuées	Référence(s)
	B_{Val}	M	V		C	D	I		
Appareils sans fil	√		√	I, S	√	√	√	E, S, s, T, C, A	GSTI 16.4.8, ITSB-02, ITSB-03, ITSB-06, ITSB-12, ITSB-15, ITSB-19, ITSB-29, ITSPSR-16, ITSPSR-17 ITSPSR-18, ITSPSR-21
Sécurité des émissions			√	I	√			E	GSTI 16.4.9, ITSD Annexe E et ITSB-18
Câbles de télécommunications			√	I, S	√	√		E	GSTI 16.4.10
Intégrité des logiciels			√	I, T, S	√	√	√	E, S, s, T, C, A	GSTI 16.4.11
Configuration des logiciels de sécurité			√	I	√	√	√	E, S, s, T, C	GSTI 16.4.11, G2-004, G2-005, ITSPSR-19 et ITSG-20
Protection contre les codes malveillants			√	I, S		√	√	E, S, s, T, C	GSTI 16.4.12 et R2-002
Détection des intrusions			√	I, S	√	√	√	E, S, s, T, C	GSTI 17-18
Protection/reprise			√	I, T, S		√		S, s, T, C, A, N	GSTI 18.5, ITSB-09 MG-01 Appendice E et MG-09 11 et 14.4
Mesures de protection opérationnelles									
Service de dépannage/résolution des problèmes			√	I, T, S	√	√	√	Toutes	GSTI 14.2 et MG-09 14.1
Gestion des incidents			√	I, T, S	√	√	√	Toutes	GSTI 12.4 et 18, MG-09 12 et ITSA-10
Évaluations des vulnérabilités			√	I, T, S	√	√	√	E, S, s, C	GSTI 12.5
Gestion des correctifs			√	I, T, S	√	√	√	E, S, s, C, A	GSTI 12.5.2
Planification de la continuité de la technologie de l'information			√	I, T, S		√		S, T, A, N	GSTI 12.8
Évaluation et vérification de la sécurité des TI			√	I, T, S	√	√	√	Toutes	GSTI 12.11 et MG-09 18
Gestion des configurations			√	I, T, S	√	√	√	Toutes	GSTI 14.1 et MG-09 14.3
Contrôle des changements			√	I, T, S	√	√	√	Toutes	GSTI 14.1
Planification de la capacité			√	I, T, S		√		S, A	GSTI 14.3
Entretien du matériel			√	I, T, S	√	√	√	A	MG-09 14.7
Protection de l'environnement			√	I, T, S		√		A, N	
Conditionnement d'alimentation/ alimentation de secours			√	I, T, S		√		S, T, A, N	
Sécurité en situations d'urgence									PGS 10.13 et NP
Plans et procédures									
Plans ministériels	√		√	Tous		√		S, T, A, N	
Essais			√	Tous		√		S, T, A, N	
Coordination avec d'autres plans			√	Tous		√		S, T, A, N	
Attribution de ressources durables			√	Tous		√		S, T, A, N	
Planification de la continuité des activités									PGS 10.14 et PCA
Structure de gouvernance									PCA 3.1 et PCCADT 3
Autorisations			√	Tous		√		S, T, C, A, N	
Responsabilités			√	Tous		√		S, T, C, A, N	

Classe de mesures Groupe de mesures Mesure de protection	Incidence			Biens protégés	Valeurs protégées			Menaces atténuées	Référence(s)
	B_{Val}	M	V		C	D	I		
Analyse des répercussions sur les activités			√	Tous		√		S, T, C, A, N	PCA 3.2 et PCCADT 4
Plans/Modalités			√	Tous		√		S, T, C, A, N	PCA 3.3 et PCCADT 5
Préparation du programme de PCA			√	Tous		√		S, T, C, A, N	PCA 3.4 et PCCADT 6
Examens, essais et vérification			√	Tous		√		S, T, C, A, N	PCA 3.4 et PCCADT 6
Enquête sur les incidents									PGS 10.15 et ESS
Enquête sur les incidents			√	Tous	√	√	√	Toutes	
Rapports d'incident			√	Tous	√	√	√	Toutes	
Sanctions									PGS 10.16 et ESS
Atteintes à la sécurité		√	√	Tous	√	√	√	E, S, s, T, C, A	
Infractions à la sécurité		√	√	Tous	√	√	√	E, S, s, T, C, A	

Nota :

1. Pour aider à sélectionner des mesures de sécurité appropriées, la liste des mesures de protection donne une indication générale des variables de risque sur lesquelles les contre-mesures ont une incidence, ainsi que des références utiles :
   - **Colonne 1** : donne la liste des mesures à l'intérieur des groupes et des classes de mesures;
   - **Colonnes 2 à 4** : indiquent celles parmi les trois variables de risque qui peuvent être atténuées par la mesure de protection, soit les valeurs des biens (B_{Val}), les menaces (M) ou, le plus fréquemment, les vulnérabilités (V);
   - **Colonne 5** : indique celles parmi les classes ou catégories de biens qui peuvent être protégées par la mesure de protection, soit le personnel (P), l'information (I), les systèmes de TI (T), les installations (INS), les services (S) ou les biens incorporels (i);
   - **Colonnes 6 à 8** : suggèrent celles parmi les valeurs de bien qui peuvent être protégées par la mesure de protection, soit la confidentialité (C), la disponibilité (D) ou l'intégrité (I);
   - **Colonne 9** : désigne certaines des activités ou classes de menaces atténuées par chacune des mesures de protection, soit l'espionnage (E), le sabotage (S), la subversion (s), le terrorisme (T), les actes criminels (C), les accidents (A) et les risques naturels (N); et
   - **Colonne 10** : inclut des références aux normes opérationnelles de sécurité de la PGS et à la documentation technique qui décrivent la mesure de protection et son utilisation prévue. Les entrées dans la colonne renvoient aux titres des documents dans la liste ci-dessous, et certaines incluent des pointeurs vers des sections particulières de la référence citée. Par exemple, PGS 10.1 renvoie à la section 10.1 de la PGS et PCCADT 3, à la section 3 des documents techniques relatifs à la PCA diffusée par SPPCC. Vous trouverez les sources de cette documentation à l'appendice G-4, Références.

- **PGS** – Politique du gouvernement sur la sécurité
- **PSST** – Politique sur la sécurité et la santé au travail
- **Normes opérationnelles de sécurité** –
  - **PCA** – Programme de planification de la continuité des activités (PCA)
  - **IB** – Identification des biens
  - **GSTI** – Gestion de la sécurité des technologies de l'information
  - **SM** – Sécurité matérielle
  - **NP** – Niveau de préparation des installations du gouvernement fédéral
  - **SGM** – Sécurité dans la gestion des marchés
  - **ESS** – Enquêtes de sécurité et sanctions
  - **FS** – Filtrage de sécurité
  - **FSA** – Formation et sensibilisation à la sécurité
- **CST – Alertes de sécurité des TI, bulletins, directives et lignes directrices**
  - **ITSA-09** – Élimination du matériel COMSEC
  - **ITSA-10** – Signalement des incidents COMSEC
  - **ITSB-02** – Évaluation de la vulnérabilité des systèmes de communication sans fil du gouvernement du Canada
  - **ITSB-03** – Tendances en matière de technologies sans fil et de sécurité des appareils sans fil
  - **ITSB-06** – Le CST approuve le BlackBerry sécurisé
  - **ITSB-09** – Fonctionnement du STU III pendant une panne d'électricité
  - **ITSB-12** – Acquisition du module de sécurité Blackberry
  - **ITSB-13** – Commande de clés pour les STE
  - **ITSB-15** – Vulnérabilité sur le plan de la sécurité présentée par les ordinateurs portatifs équipés de la technologie WLAN
  - **ITSB-18** – Liste des produits recommandés par l'OTAN (NRPL) – produits TEMPEST homologués
  - **ITSB-19** – Mesures de sécurité – appareils électroniques sans fil
  - **ITSB-29** – Offre à commandes concernant le module de sécurité GSM (Global System for Mobile Communication) SECTERA (SGSM)
  - **ITSD-01** – Directives sur l'application de la sécurité des communications au sein du gouvernement du Canada
  - **ITSD-02** – Exigences sécuritaires de base en matière de zones de sécurité TI
  - **ITSG-06 –** Effacement et déclassification des supports d'information électroniques
  - **ITSG-10 –** Manuel de contrôle du matériel COMSEC
  - **ITSG-13 –** Manuel sur la commande de clés cryptographiques
  - **ITSG-20 –** Sécurité de base recommandée pour Windows Server 2003
  - **ITSPSR-14 –** Projet de télétravail
  - **ITSPSR-16 –** Évaluation de la vulnérabilité des Services de communications personnelles (SCP) et des systèmes cellulaires

- **ITSPSR-17 –** Évaluation des vulnérabilités de Bluetooth
- **ITSPSR-18 –** Évaluation des vulnérabilités des assistants numériques personnels (PDA)
- **ITSPSR-19 –** Sécurité de base recommandée pour Windows 2000 Pro et X Pro
- **ITSPSR-21 –** Évaluation de la vulnérabilité des réseaux locaux (LAN) sans fils 802.11
- **MG-1 –** Sécurité des réseaux, analyse et mise en oeuvre
- **MG-2 –** Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information
- **MG-4 –** Guide de certification et d'accréditation des technologies de l'information
- **MG-9 –** Manuel canadien de la sécurité des technologies de l'information

▪ **MAECI** – Avertissements en matière de voyage

▪ **Sécurité publique et Protection civile Canada (SPPCC)**
- **PCCADT** – Programme de planification de la continuité des activités – Documents techniques

▪ **Travaux publics et Services gouvernementaux Canada –**
- **MSI** – Manuel de la sécurité industrielle

▪ **GRC – Guides, bulletins et rapports sur la sécurité matérielle et la sécurité des TI**
- **G1-001** – Guide d'équipement de sécurité
- **G1-002** – Éclairage de sécurité
- **G1-003** – Vitrage
- **G1-004** – Construction d'une aire protégée
- **G1-005** – Guide pour la préparation d'un énoncé de sécurité matérielle
- **G1-006** – Cartes d'identité / Insignes d'accès
- **G1-007** – Scellage de protection des clés d'urgence et passe-partout ou des serrures à code d'immeubles
- **G1-008** – Lignes directrices visant les services de gardiens
- **G1-009** – Norme pour le transport ou la transmission de renseignements et de biens de nature délicate
- **G1-010** – Éléments du Code national du bâtiment 1995 touchant la sécurité
- **G1-011** – Devis de construction de portes escamotables en plafond
- **G1-013** – Besoins en espace des centres de surveillance
- **G1-014** – Devis de construction d'une barrière pour échelle extérieure
- **G1-015** – Contrôle des accès, portes basculantes
- **G1-016** – Les systèmes de clés maîtresses
- **G1-017** – Quincaillerie
- **G1-018** – Portes et cadres de portes
- **G1-019** – Chambres fortes
- **G1-024** – Contrôle de l'accès
- **G1-025** – Protection, détection et intervention
- **G1-026** – Établissement des zones de sécurité matérielle

- **G1-027** – Responsabilités des ministères gardiens et des ministères locataires en matière de sécurité matérielle
- **G1-029** – Pièces sécuritaires
- **G1-030** – Guide de sensibilisation à la sécurité
- **G1-031** – Pièces pour serveurs
- **G2-002** – Guide sur la répression des vols de matériel informatique
- **G2-003** – Lignes directrices sur l'élimination et la destruction des renseignements protégés sur disques durs
- **G2-004** – Guide de configuration de sécurité avancée pour Windows 2000 Professional
- **G2-005** – Guide de configuration de sécurité du Active Directory de Windows 2000
- **B2-001** – Produits de remplacement pour DSX
- **R2-001** – Les technologies biométriques
- **R2-002** – Logiciels malveillants : les tendances qui se dessinent
- **DSX-G** – Manuel de l'utilisateur pour le logiciel de réécriture de disque dur (DSX) de la GRC

2. On doit utiliser la liste des mesures de protection avec prudence puisqu'elle ne saurait être exhaustive et qu'il existe des exceptions pour plusieurs entrées. On la recommande toutefois comme point de départ utile pour l'analyse au cours du processus de sélection des mesures de protection de la phase des recommandations d'un projet d'EMR. Cela dit, d'autres documents seront ajoutés au fur et à mesure. Toute suggestion de références supplémentaires doit être portée à l'attention des bureaux mentionnés dans l'Avant-propos.

Appendice F-3 – Sélection des mesures de protection potentielles

1 Généralités

Dans le but de déterminer un ensemble approprié de mesures de sécurité pour les recommandations finales d'un rapport d'EMR, on peut appliquer plusieurs critères de sélection de mesure de protection en deux volets :

- premièrement, déterminer des solutions potentielles pour tous les risques résiduels évalués inacceptables; et
- deuxièmement, évaluer leur efficacité relative comme mécanismes de réduction des risques.

Ensuite, au cours du processus suivant d'EMR, résumé à l'appendice F-4, on calcule les coûts comparatifs afin de déterminer les options les plus rentables.

2 Déterminer les solutions potentielles

Les mesures possibles de protection sont identifiées en six étapes, comme suit :

- **Étape 1.** Extraire tous les risques résiduels inacceptables de la liste des risques résiduels évalués, à l'appendice E-2.
- **Étape 2.** Déterminer quels biens sont menacés et leurs valeurs, habituellement au niveau du groupe ou du sous-groupe de biens, et occasionnellement en tenant compte de composants ou d'éléments individuels particuliers.
- **Étape 3.** Déterminer les menaces, normalement aux niveaux des catégories d'activité de menace ou d'agent de menace, qui posent des risques inacceptables, et les niveaux de ces menaces.
- **Étape 4.** Déterminer les vulnérabilités qui exposent ces biens à des compromissions, et les niveaux de ces vulnérabilités.
- **Étape 5.** Pour permettre une analyse plus approfondie, copier ces données dans une liste abrégée de risques résiduels évalués, illustrée au tableau F3-1. Entrer tous les biens pour lesquels il existe des risques inacceptables dans la première colonne, et leurs valeurs dans la seconde. Ensuite, pour chaque bien, produire la liste de toutes les menaces connexes, et de leurs niveaux, qui posent des risques inacceptables dans les colonnes trois et quatre, respectivement. Pour chacune de ces menaces, entrer dans les colonnes cinq et six toutes les vulnérabilités connexes, et leurs niveaux, qui exposent le bien à des risques inacceptables. Enfin, entrer dans la septième colonne les niveaux inacceptables de risque résiduel évalué. Cette tâche peut être accomplie rapidement et efficacement en classant successivement la liste des risques résiduels évalués de l'appendice E-2 en ordre des colonnes Bien, Menace connexe et Vulnérabilité connexe.

Biens exposés à un risque inacceptable		Menaces causant des risques inacceptables		Vulnérabilités exposant les biens à des risques inacceptables		R
Bien	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	

Tableau F3-1 : Liste abrégée des risques résiduels évalués

- **Étape 6.** Une fois que l'on connaît les biens, les menaces et les vulnérabilités à l'origine des risques résiduels inacceptables, on peut examiner la liste des mesures de protection à l'appendice F-2 et identifier les mesures de sécurité potentielles en se fondant sur les biens qu'elles protègent, les menaces qu'elles prennent en considération et les vulnérabilités qu'elles atténuent.

3 Évaluer l'efficacité des mesures de protection

On évalue ensuite l'efficacité de chaque mesure de protection éventuelle en six étapes, comme suit :

- **Étape 1.** Calculer la différence de niveaux des valeurs initiales et des valeurs réduites de certains mécanismes d'évitement, plus particulièrement ceux qui limitent les valeurs des biens.
- **Étape 2.** Évaluer l'incidence globale sur les niveaux de menace de toute mesure d'évitement qui réduit la probabilité d'un incident, de tout mécanisme dissuasif qui influe sur les intentions de l'agent de menace et de toute mesure préventive qui a une incidence sur les capacités de celui-ci.
- **Étape 3.** Déterminer les effets (probabilité de compromission ou gravité du résultat) sur les vulnérabilités connexes de la plupart des mesures préventives et sur tous les mécanismes de détection, d'intervention et de reprise.
- **Étape 4.** En utilisant les niveaux révisés des valeurs de biens, des menaces et des vulnérabilités, recalculer les risques résiduels dans la liste abrégée des risques résiduels évalués afin de déterminer si les mesures de protection proposées permettent ou non d'atteindre des niveaux de risque acceptables.
- **Étape 5.** Pour chaque mesure de protection qui permet de ramener les risques inacceptables à des niveaux acceptables, évaluer les incidences de critères de sélection secondaires, plus particulièrement leur acceptabilité, leur visibilité, leur vulnérabilité, leur interdépendances avec d'autres mesures de sécurité, le degré d'intervention humaine qu'ils requièrent, leur sensibilité, leur maturité et leur conformité aux normes de sécurité. Un ou plusieurs de ces facteurs peuvent déterminer le choix final entre deux options également acceptables.
- **Étape 6.** Ensuite, effectuer une analyse coûts-avantages de tous les choix acceptables qui permettent d'atteindre les niveaux de risque cibles au cours du processus suivant d'EMR, décrit à l'appendice F-4.

4 Exemple

4.1 Bureaux de relations de travail

Quatre agents des relations de travail d'un petit organisme gouvernemental sont chargés d'enquêter sur des griefs présentés par des employés et de recommander des solutions appropriées à la direction; cette responsabilité pourrait permettre d'identifier plusieurs risques dans un rapport d'EMR en se fondant sur les valeurs des biens, les menaces et les vulnérabilités définies ci-dessous :

- **Valeurs des biens.** Par définition, les quatre agents justifient une valeur intrinsèque élevée si l'on tient compte de la possibilité de menaces de violence. Leurs rapports d'enquête seront probablement cotés Protégé B, valeur de confidentialité moyenne. Les modifications non autorisées ou la falsification de preuve signalées dans ces rapports pourraient causer un profond embarras à certaines personnes, d'où l'attribution d'une valeur d'intégrité moyenne.
- **Menaces.** Si des employés avaient harcelé ou menacé physiquement les agents des relations de travail à deux ou trois occasions durant les entrevues au cours de la dernière année, on attribuerait à la menace une cote moyenne en fonction de la fréquence passée (100 à 1 000 jours) et des capacités de l'agent de menace (connaissances, compétences et ressources moyennes). Si d'autres employés avaient tenté de lire les dossiers subrepticement et d'en trafiquer le contenu au cours de la même période, les deux menaces seraient également cotées au niveau moyen.
- **Vulnérabilités.** Si les entrevues ont été menées dans des aires ouvertes, facilement accessibles à tous les autres employés, la totale facilité d'accès pourrait s'avérer un mécanisme préventif très faible. Si cette vulnérabilité était combinée à des mesures inadéquates de détection et d'intervention, par exemple des communications d'urgence déficientes ou l'absence de système d'alarme, des visiteurs non escortés se promenant librement dans les locaux et un poste de gardien de sécurité éloigné, la cote globale de la vulnérabilité liée aux menaces de harcèlement ou d'agression pourrait être très élevée. L'environnement à aire ouverte et l'accès aux locaux sans escorte pourraient également faciliter les menaces de furetage et de trafiquage de dossiers sensibles. De plus, si les agents des relations de travail avaient tendance à laisser les bureaux sans aucune surveillance ni supervision, la probabilité de détection de divulgation non autorisée pourrait être très faible. L'absence de contrôles d'intégrité quelconques rendrait également difficile la détection de toute modification non autorisée des rapports et recommandations. Dans les deux cas, l'incapacité de détecter les menaces possibles et d'y réagir, associée à des contrôles d'accès inadéquats, donnerait lieu à des vulnérabilités de niveau très élevé.
- **Risques résiduels évalués.** Dans chaque cas, les risques résiduels évalués associés à ces valeurs de biens, à ces menaces et à ces vulnérabilités se situent dans la gamme de risques élevés, un niveau inacceptable. Cette évaluation doit être présentée dans une feuille de travail de sélection de mesure de protection, tel qu'il est expliqué aux étapes 1 à 5 du premier volet du processus de sélection des mesures de protection et illustré dans le tableau F3-2, Liste des risques résiduels évalués inacceptables.

Biens exposés à un risque inacceptable				Menaces causant des risques inacceptables		Vulnérabilités exposant les biens à des risques inacceptables		R
Bien	B_{Val}			Menace	M	Vulnérabilité	V	
	C	D	I					
Agents des relations de travail		E		Harcèlement/Agression	M	Aire ouverte	TE	E
		E			M	Aucune alarme	TE	E
		E			M	Aucune unité d'intervention	TE	E
Dossiers de griefs	M			Furetage des employés	M	Aire ouverte	TE	E
	M				M	Accès non supervisé	TE	E
			M	Falsification de preuve	M	Aire ouverte	TE	E
			M		M	Accès non supervisé	TE	E
			M		M	Contrôles d'intégrité déficients	TE	E

Tableau F3-2 : Liste des risques résiduels évalués inacceptables

4.2 Déterminer les solutions potentielles

Après avoir isolé les risques résiduels inacceptables aux fins d'examen, on peut examiner la liste des mesures de protection de l'appendice F-2 afin de déterminer des mesures de sécurité potentielles capables de protéger les biens, c.-à-d., les agents des relations de travail (personnel) et les dossiers de griefs (documents ayant des valeurs à la fois de confidentialité et d'intégrité), menacés par des risques de violence, de furetage et de falsification de preuve, et de déterminer les vulnérabilités connexes. Dans le cas qui nous occupe plus particulièrement, certaines des considérations pertinentes pourraient inclure les éléments suivants :

- **Valeurs des biens.** Compte tenu de la nature des biens, personnel et documents sensibles, on ne peut mettre en place de mesures d'évitement pour limiter la valeur des biens.
- **Menaces.** Certaines mesures de protection, tels des panneaux de mise en garde, peuvent dissuader les employés violents et ceux qui cherchent à lire ou modifier les dossiers de grief; toutefois, on ne peut presque rien faire concernant les capacités des agents de menace (connaissances, compétences et ressources).
- **Vulnérabilités.** De toute évidence, dans ce cas particulier, l'approche la plus profitable consiste à cibler les différentes vulnérabilités, soit les faibles mécanismes de prévention, de détection et d'intervention, qui contribuent aux risques résiduels inacceptables.
- **Mesures de protection potentielles.** Certaines options peuvent inclure des mesures de protection qui figurent dans la liste du tableau F3-3, et qui sont décrites ci-dessous durant l'évaluation de l'efficacité des mesures.

4.3 Évaluer l'efficacité des mesures de protection

La présence de gardiens de sécurité sur place peut avoir un certain effet dissuasif, bien qu'il soit difficile de mesurer avec précision l'incidence réelle de cette présence sur les intentions de l'agent de menace. D'autre part, les mesures de protection potentielles n'atténuent ni les valeurs des biens ni les menaces mais uniquement les vulnérabilités, soit la probabilité de compromission ou la gravité du résultat. Ainsi, pour ce scénario particulier, la réduction globale des niveaux de vulnérabilité est le principal indicateur de l'efficacité des mesures de protection. De plus, pour atteindre des risques résiduels projetés moyens, niveau généralement acceptable, les mesures de protection proposées doivent permettre de réduire à une faible niveau toutes les vulnérabilités de niveau très élevé associées au harcèlement et aux agressions, et à un niveau moyen les vulnérabilités associées au furetage et au trafiquage. On étudie brièvement ci-dessous l'incidence prévue de chaque mesure de sécurité.

- **Entrée verrouillée.** Une porte verrouillée à l'entrée des locaux du bureau de relations de travail constitue une mesure préventive moyennement efficace qui restreint l'accès tant au personnel qu'aux dossiers de grief. Toutefois, sans une amélioration complémentaire des mesures de détection, d'intervention et de reprise, ce mécanisme simple de contrôle d'accès est en mesure de réduire la vulnérabilité globale de Très élevée (probabilité de compromission et gravité des résultats élevées) à Élevée (probabilité moyenne de compromission, mais gravité élevée des résultats). Lorsque ces mesures sont combinées à d'autres mesures de protection, notamment la formation du personnel, un avertisseur individuel et une unité d'intervention spécialisée, la vulnérabilité globale peut chuter à un niveau moyen ou même faible.
- **Accès avec escorte.** L'entrée verrouillée ne peut être que moyennement efficace comme mécanisme de prévention puisque les clients légitimes que l'on doit accueillir pour des entrevues et du counselling sont susceptibles de harceler le personnel ou de tenter d'accéder aux dossiers de grief. Accompagner tous les visiteurs durant leur visite peut empêcher la plupart des tentatives de furetage et de trafiquage, mais probablement pas le harcèlement ni les menaces de violence. L'accès supervisé offre également une capacité efficace de détection et d'intervention pour les trois menaces et, à ce titre, cette seule mesure de protection peut réduire le niveau Très élevé de la vulnérabilité liée au harcèlement et aux agressions à un niveau Élevé (probabilité de compromission et gravité des résultats élevées) ou même Moyen (probabilité toujours élevée de compromission, mais gravité moyenne ou même faible des résultats). L'accès avec escorte, qui sert à la fois de mesure préventive et de mécanisme de détection et d'intervention pour les activités de furetage et de trafiquage, est encore plus efficace contre ces menaces puisqu'il réduit les vulnérabilités connexes à un niveau Très faible (probabilité de compromission et gravité des résultats faibles). Évidemment, l'efficacité de cette mesure de protection est susceptible de diminuer avec le temps si les accompagnateurs deviennent moins vigilants.
- **Formation du personnel.** La formation et la sensibilisation du personnel concernant la capacité d'identifier, de signaler et de contrer les problèmes réels et potentiels sont essentielles à l'application efficace des autres mesures de protection (entrée verrouillée, accès avec escorte et politique de rangement du bureau). Pour mieux refléter l'incidence ultime de cette formation sur les niveaux de vulnérabilité, on doit effectuer une

évaluation de l'efficacité relative des autres mesures de protection liées à la mise en place et à l'intervention du personnel responsable.

Options de mesure de protection	Fonctions de sécurité	Biens protégés	Menaces atténuées	Vulnérabilités prises en compte
Entrée verrouillée	Prévention	Employés	Harcèlement/Agression	Aire ouverte
		Dossiers de griefs	Furetage	Aire ouverte
		Dossiers de griefs	Trafiquage	Aire ouverte
Accès avec escorte	Prévention	Dossiers de griefs	Furetage	Accès non supervisé
		Dossiers de griefs	Trafiquage	Accès non supervisé
	Détection	Employés	Harcèlement/Agression	Aucune alarme
		Dossiers de griefs	Furetage	Accès non supervisé
		Dossiers de griefs	Trafiquage	Accès non supervisé
	Intervention	Employés	Harcèlement/Agression	Aucune unité d'intervention
		Dossiers de griefs	Furetage	Aucune unité d'intervention
		Dossiers de griefs	Trafiquage	Aucune unité d'intervention
Formation du personnel	Prévention	Employés	Harcèlement/Agression	Accès non supervisé
		Dossiers de griefs	Furetage	Accès non supervisé
		Dossiers de griefs	Trafiquage	Accès non supervisé
	Détection	Employés	Harcèlement/Agression	Aucune alarme
		Dossiers de griefs	Furetage	Accès non supervisé
		Dossiers de griefs	Trafiquage	Accès non supervisé
	Intervention	Employés	Harcèlement/Agression	Aucune unité d'intervention
		Dossiers de griefs	Furetage	Aucune unité d'intervention
		Dossiers de griefs	Trafiquage	Aucune unité d'intervention
Politique en matière de rangement du bureau	Prévention	Dossiers de griefs	Furetage	Accès non supervisé
		Dossiers de griefs	Trafiquage	Accès non supervisé
Salles d'entrevue sécurisées	Prévention	Employés	Harcèlement/Agression	Aire ouverte
Avertisseur individuel	Détection	Employés	Harcèlement/Agression	Aucune alarme
Gardien de sécurité en devoir	Dissuasion	Employés	Harcèlement/Agression	Accès non supervisé
		Dossiers de griefs	Furetage	Accès non supervisé
		Dossiers de griefs	Trafiquage	Accès non supervisé
	Prévention	Employés	Harcèlement/Agression	Accès non supervisé
	Détection	Employés	Harcèlement/Agression	Aucune alarme
	Intervention	Employés	Harcèlement/Agression	Aucune unité d'intervention
		Dossiers de griefs	Furetage	Aucune unité d'intervention
		Dossiers de griefs	Trafiquage	Aucune unité d'intervention
Gardien de sécurité sur appel	Intervention	Employés	Harcèlement/Agression	Aucune unité d'intervention
		Dossiers de griefs	Furetage	Aucune unité d'intervention
		Dossiers de griefs	Trafiquage	Aucune unité d'intervention
Télévision en circuit fermé	Détection	Employés	Harcèlement/Agression	Aucune alarme
Numéros séquentiels aux entrées des dossiers	Détection	Dossiers de griefs	Trafiquage	Contrôles d'intégrité déficients
Fichiers en double	Reprise	Dossiers de griefs	Trafiquage	Contrôles d'intégrité déficients

Tableau F3-3 : Liste des mesures de protection potentielles

- **Politique en matière de rangement du bureau.** La politique en matière de rangement du bureau, qui exige des employés qu'ils verrouillent les dossiers sensibles qu'ils n'utilisent pas dans des conteneurs de sécurité, offre un moyen simple mais efficace d'empêcher tout accès non autorisé aux fins de furetage ou de trafiquage. Même sans mesures de détection et d'intervention complémentaires, cette mesure de protection peut réduire le niveau de la vulnérabilité de Très élevé (probabilité de compromission et gravité des résultats élevées) à Moyen (faible probabilité de compromission, mais gravité élevée des résultats). Puisque ces procédures représentent certains inconvénients pour le personnel, celui-ci peut regimber ou ne pas se conformer consciencieusement à ces mesures et, de ce fait, en miner l'efficacité.
- **Salles d'entrevue sécurisées.** Les salles d'entrevue sécurisées, avec leurs divisions en verre incassable et leurs entrées distinctes pour le personnel et les clients, constituent des mesures de protection très efficaces contre la violence physique. La solidité de leur construction, en plus d'aider à restreindre les dommages en cas de confrontation, représente un mécanisme d'intervention partielle qui permet de réduire le niveau des vulnérabilités liées au harcèlement et aux agressions de Très élevé (probabilité de compromission et gravité des résultats élevées) à Faible (faible probabilité de compromission et gravité moyenne des résultats). L'installation éventuelle d'un avertisseur individuel pour alerter une unité d'intervention rapide pourrait ultimement réduire le niveau des vulnérabilités à Très faible.
- **Gardien de sécurité en devoir.** L'affectation d'un gardien de sécurité dans le bureau de relations de travail pourrait contrer plusieurs vulnérabilités liées aux menaces de harcèlement et d'agression. Par exemple, un gardien qui a reçu une formation appropriée peut être en mesure de reconnaître les situations potentiellement dangereuses et d'intercepter toute personne suspecte, ou de venir en aide aux visiteurs agités pour les calmer, toutes des mesures préventives qui sont très efficaces. Il peut également remplir des fonctions de détection et d'intervention pour atténuer tout risque de blessures potentielles infligées par des clients abusifs ou violents. Cette mesure permettrait donc de réduire le niveau des vulnérabilités globales de Très élevé (probabilité de compromission et gravité des résultats élevées) à Faible et même à Très faible (faible probabilité de compromission et gravité moyenne ou faible des résultats).
- **Gardien de sécurité sur appel.** De toute évidence et pour plusieurs raisons, un gardien de sécurité sur appel est moins efficace qu'un gardien en devoir dans le bureau de relations de travail. Dans un premier temps, un gardien qui n'est pas sur place ne peut remplir de fonctions de prévention ni de détection. Deuxièmement, ce gardien est en mesure d'intervenir uniquement si d'autres mécanisme quelconque de détection déclenchent une alerte. Enfin, il est possible que le gardien puisse intervenir moins rapidement et moins efficacement, selon l'emplacement de son poste de garde. L'intervention d'un gardien de sécurité assigné à un poste de garde centralisé, combinée à une mesure de prévention moyennement efficace, par exemple, une entrée verrouillée et un mécanisme de détection tel un avertisseur individuel, peut contribuer à réduire le niveau de la vulnérabilité globale liée à la violence en milieu de travail de Très élevé (probabilité de compromission et gravité des résultats élevées) à Moyen (probabilité de compromission et gravité des résultats moyennes).

- **Télévision en circuit fermé.** Un système de télévision en circuit fermé (TVCF), pour autant qu'il soit contrôlé à partir d'un poste de garde central, peut offrir un mécanisme de détection très efficace, notamment dans le cas de clients agités ou potentiellement abusifs. Combinée à une capacité d'intervention rapide, cette mesure de protection ne peut empêcher les situations de harcèlement ou d'agression, mais pourrait aider à contrôler les incidents et ainsi réduire le niveau de gravité des résultats de Élevé à Moyen ou même à Faible. Une mesure préventive complémentaire, telle une entrée verrouillée, qui réduirait le niveau de probabilité de compromission de Élevé à Moyen ferait en sorte de réduire le niveau de vulnérabilité globale de Très élevé à Moyen ou Faible. Nonobstant l'efficacité potentielle de l'équipement de TVCF, les préoccupations qu'il soulève au plan de la protection de la vie privée et la résistance des employés à toute surveillance permanente pourraient jouer contre son installation.
- **Numéros séquentiels.** L'attribution d'un numéro séquentiel à chaque entrée des dossiers de griefs ne peut empêcher le trafiquage; par contre, cette pratique peut aider à déceler certaines altérations, par exemple, la suppression d'une preuve importante. Sans mesure préventive correspondante, toutefois, cette mesure de protection moyennement efficace peut uniquement réduire le niveau de vulnérabilité connexe de Très élevé (probabilité de compromission et gravité des résultats élevées) à Élevé (probabilité élevée de compromission et gravité moyenne des résultats). En outre, les agents des relations de travail peuvent trouver ces procédures laborieuses et fastidieuse et résister à leur instauration.
- **Fichiers en double.** Les numéros séquentiels peuvent aider à déceler toute modification non autorisée des dossiers de grief; cependant, ils contribuent peu à faciliter la reprise après un incident réel. La tenue de dossiers parallèles ou en double peut s'avérer raisonnablement efficace comme stratégie de sauvegarde et de reprise. Ici encore, sans mesure préventive correspondante, tels des numéros de dossier, l'incidence de cette mesure de protection sur la vulnérabilité est limitée. Les dossiers en double prêtent également le flanc à des problèmes d'intégrité puisque les deux versions peuvent ne pas correspondre si elles ne sont pas scrupuleusement tenues à jour.

4.4 Sommaire des options

Pour être en mesure d'atteindre les niveaux cibles de risque, il sera nécessaire de réduire le niveau des vulnérabilités de manière substantielle, soit, au minimum, de Très élevé à Moyen, tel qu'il a été indiqué précédemment. On doit donc choisir des mesures de protection complémentaires pour réduire tant la probabilité de compromission (par des mesures préventives) que la gravité des résultats (par des mécanismes de détection, d'intervention et même de reprise). Les combinaisons de mesures de sécurité qui suivent, tirées du tableau F3-3 et qui doivent toutes faire l'objet d'une formation adéquate, peuvent répondre à ces exigences :

- **Entrée verrouillée et accès avec escorte.** Combinées, ces mesures de protection peuvent être moyennement efficaces comme mesures préventives contre le harcèlement et les agressions (probabilité moyenne de compromission) et très efficaces contre les activités de furetage et de trafiquage (faible probabilité de compromission). En plus, l'accès avec escorte et la formation en sécurité peuvent offrir des capacités efficaces de détection et d'intervention contre toutes les menaces (faible gravité des résultats), à

l'exception peut-être des menaces de harcèlement et d'agression pour lesquelles un employé peut hésiter à intervenir et se contenter d'effectuer un appel à l'aide. Dans ce dernier cas, le niveau de vulnérabilité passerait à Moyen (probabilité de compromission et gravité des résultats moyennes). Si l'on prend en considération l'ensemble de ces problèmes, le niveau des vulnérabilités globales liées au harcèlement et aux agressions baisserait à Faible ou Moyen et celui des vulnérabilités globales liées au furetage et au trafiquage, à Très faible. Vous trouverez au tableau F3-4 un sommaire des risques résiduels projetés advenant que ces mesures de protection soient approuvées et instaurées.

Biens exposés à un risque inacceptable		**Menaces causant des risques inacceptables**		**Vulnérabilités exposant les biens à des risques inacceptables**		**R**
Bien	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	
Agents des relations de travail	E	Harcèlement/Agression	M	Aire ouverte	F-M	M-E
	E		M	Aucune alarme	F-M	M-E
	E		M	Aucune unité d'intervention	F-M	M-E
Dossiers de griefs	M	Furetage des employés	M	Aire ouverte	TF	F
	M		M	Accès non supervisé	TF	F
	M	Falsification de preuve	M	Aire ouverte	TF	F
	M		M	Accès non supervisé	TF	F

Tableau F3-4 : Risques résiduels projetés - Entrée verrouillée et accès avec escorte

- **Ajout d'un avertisseur individuel et d'un gardien de sécurité sur appel.**
  Dans l'option précédente, si l'intervention d'un employé en situation de harcèlement ou d'agression soulève de sérieuses préoccupations, on peut prévoir l'ajout d'un avertisseur individuel pour alerter un gardien de sécurité formé adéquatement et ainsi obtenir une capacité d'intervention plus efficace qui permet de réduire le niveau des vulnérabilités à faible (probabilité moyenne de compromission et faible gravité des résultats). Les résultats sont indiqués dans le tableau F3-5.

Biens exposés à un risque inacceptable		Menaces causant des risques inacceptables		Vulnérabilités exposant les biens à des risques inacceptables		R
Bien	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	
Agents des relations de travail	E	Harcèlement/Agression	M	Aire ouverte	F	M
	E		M	Aucune alarme	F	M
	E		M	Aucune unité d'intervention	F	M
Dossiers de griefs	M	Furetage des employés	M	Aire ouverte	TF	F
	M		M	Accès non supervisé	TF	F
	M	Falsification de preuve	M	Aire ouverte	TF	F
	M		M	Accès non supervisé	TF	F

Tableau F3-5 : Risques résiduels projetés - Ajout d'un avertisseur individuel et d'un gardien de sécurité sur appel

- **Gardien de sécurité en devoir, politique en matière de rangement du bureau et numéros séquentiels.** Un gardien de sécurité bien formé est en mesure d'affronter de manière très efficace toutes les vulnérabilités liées au harcèlement et aux agressions, en assurant à la fois un service de prévention et un mécanisme de détection et d'intervention, et, ainsi, de réduire le niveau des vulnérabilités de Très élevé (probabilité de compromission et gravité des résultats élevées) à Très faible (probabilité de compromission et gravité des résultats faibles). La politique en matière de rangement du bureau peut empêcher la plupart des activités de furetage et de trafiquage liées aux dossiers de grief, alors que l'attribution de numéros séquentiels aux entrées des dossiers peut être moyennement efficace pour déceler les modifications non autorisées. Ainsi, le niveau des vulnérabilités liées au furetage peut passer de Très élevé (probabilité de compromission et gravité des résultats élevées) à Moyen (faible probabilité de compromission mais gravité élevée des résultats), et celui des vulnérabilités liées au trafiquage, de Très élevé (probabilité de compromission et gravité des résultats élevées) à Faible (faible probabilité de compromission et gravité moyenne des résultats). Ces incidences sont indiquées dans le tableau F3-6.

Biens exposés à un risque inacceptable		Menaces causant des risques inacceptables		Vulnérabilités exposant les biens à des risques inacceptables		R
Bien	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	
Agents des relations de travail	E	Harcèlement/Agression	M	Aire ouverte	TF	F
	E		M	Aucune alarme	TF	F
	E		M	Aucune unité d'intervention	TF	F
Dossiers de griefs	M	Furetage des employés	M	Aire ouverte	M	M
	M		M	Accès non supervisé	M	M
	M	Falsification de preuve	M	Aire ouverte	F	M
	M		M	Accès non supervisé	F	M

Tableau F3-6 : Risques résiduels projetés - Gardien de sécurité, etc.

- **Salles d'entrevue sécurisées.** Dans l'option précédente, on peut substituer au gardien de sécurité une salle d'entrevue sécurisée et obtenir la même incidence sur les vulnérabilités liées au harcèlement et aux agressions, notamment une réduction du niveau de vulnérabilité de Très élevé (probabilité de compromission et gravité des résultats élevées) à Très faible (faible probabilité de compromission et faible gravité des résultats). Une politique en matière de rangement du bureau et l'attribution de numéros séquentiels aux entrées des dossiers peuvent contrer les vulnérabilités liées au furetage et au trafiquage. Cette combinaison peut permettre d'obtenir la même incidence globale sur les vulnérabilités et les risques résiduels projetés que l'option précédente dans le tableau F3-6.
- **Équipement de télévision en circuit fermé (TVCF).** Comme mesure de détection, l'équipement de TVCF ne peut réduire les vulnérabilités liées au harcèlement et aux agressions sans un mécanisme d'intervention complémentaire, tel un gardien possédant une formation adéquate. L'avertisseur individuel mentionné dans la seconde option permet d'obtenir les mêmes résultats de manière plus fiable; on ne doit donc pas tenir compte de la surveillance en circuit fermé au cours de l'évaluation subséquente de la rentabilité des mesures de protection.

4.5 Conclusion

Les quatre options décrites ci-dessus représentent des regroupements raisonnables de mesures de protection, tant au plan des mesures préventives que des mécanismes de détection et d'intervention. De toute évidence, il ne s'agit pas des seules possibilités mais plutôt de combinaisons réalistes, chacune permettant d'atteindre ou de dépasser la gamme cible de risques résiduels, notamment des niveaux moyens ou inférieurs. Le meilleur choix sera déterminé au cours du processus suivant de la phase de recommandations d'un projet d'EMR, soit l'identification des coûts connexes et l'évaluation de la rentabilité, expliquées plus en détails à l'appendice F-4.

Page intentionnellement laissée en blanc

Appendice F-4 – Calcul de la rentabilité des mesures de protection

1 Généralités

Pour déterminer laquelle des options identifiées au cours du processus d'EMR précédent, Sélection des mesures de protection potentielles, offre le meilleur rapport qualité-prix, on peut effectuer une analyse coûts-avantages en deux volets :

- premièrement, estimer le coût total de possession de chaque combinaison de mesures de protection; et
- deuxièmement, calculer leur rentabilité en fonction de la réduction globale des risques pour chaque dollar dépensé.

Ensuite, les solutions les plus rentables peuvent être présentées dans les recommandations finales à la direction aux fins d'évaluation et d'approbation, de financement et de mise en œuvre subséquente, tel que décrit à l'appendice F-5.

2 Déterminer le coût total de possession

On effectue la projection du coût total de possession de chaque option viable en trois étapes, comme suit :

- **Étape 1.** Calculer les coûts directs des mesures de protection proposées, incluant les dépenses liées à la conception et au développement, à l'acquisition, à l'intégration, à l'installation, à la documentation, à la formation, aux activités courantes et à l'entretien, selon le cas.
- **Étape 2.** Estimer les coûts et les avantages indirects attribués aux mesures de sécurité proposées en fonction de la productivité réduite et de l'efficacité accrue respectivement.
- **Étape 3.** Calculer le coût total de possession de chaque proposition, qui est la somme de tous les coûts directs et indirects et des avantages indirects.

3 Évaluer la rentabilité des mesures de protection

On calcule la rentabilité comparative de chacune de ces options en trois étapes, comme suit :

- **Étape 1.** Évaluer la durée utile prévue de la mesure de protection proposée et calculer le coût annuel amorti, soit le coût total de possession divisé par la durée utile prévue.
- **Étape 2.** Calculer la réduction totale des risques de chaque mesure de sécurité potentielle :
  - sélectionner dans l'appendice E-2 toutes les combinaisons de risques inacceptables (valeur du bien, menace et vulnérabilité) atténuées par la mesure de protection proposée;

  - recalculer le risque résiduel de chacune de ces entrées en fonction de la plus faible valeur de bien, menace ou vulnérabilité réalisée par la mesure de protection proposée;
  - déterminer le nombre de niveaux entre les risques évalués et les risques résiduels projetés de chaque combinaison visée par la mesure de protection proposée; et
  - calculer la réduction totale des risques, c.-à-d., la somme de tous les changements de niveaux de risques.
- **Étape 3.** Calculer la rentabilité de chaque proposition, soit le coût annuel amorti divisé par la réduction totale des risques.

4 Exemple

4.1 Bureaux des relations de travail

L'exemple présenté à l'appendice F-3 pour illustrer la sélection des mesures de protection potentielles visant à protéger les agents des relations de travail et leurs dossiers de griefs peut être complété par l'évaluation (ci-dessous) des coûts connexes et de la rentabilité pour chacune des options suivantes :

- **Option 1.** Entrée verrouillée combinée à un accès avec escorte et une formation en sécurité.
- **Option 2.** Ajout d'un avertisseur individuel et d'un gardien de sécurité sur appel à l'option 1.
- **Option 3.** Gardien de sécurité en devoir avec une politique en matière de rangement du bureau et des numéros séquentiels de dossier.
- **Option 4.** Remplacement des gardiens de sécurité par des salles d'entrevue sécurisées dans l'option 3.

4.2 Coût total de possession

Le tableau F4-1 ci-dessous inclut un sommaire des coûts types représentatifs associés à chacune des quatre options.

Coûts	Option 1	Option 2	Option 3	Option 4
Conception/Développement	–	–	–[1]	5 000 $[2]
Acquisition	500 $[3]	1 300 $[4]	750 $[5]	10 400 $[6]
Intégration	–	–	–	–
Installation	250 $[7]	850 $[8]	150 $[9]	16 300 $[10]
Documentation	300 $[11]	500 $[12]	300 $[13]	200 $[14]
Formation	400 $[15]/100 $[16]	500 $[17]/125 $[18]	200 $[19]/100 $[20]	100 $[21]/25 $[22]
Activités courantes	–	–[23]	37 500 $[24]	–

1 Nous présumons qu'il y a de l'espace à l'entrée pour installer un poste de garde et qu'aucun réaménagement n'est requis.
2 Production des conceptions et des plans architecturaux.
3 Achat d'une serrure de porte à clavier pour faciliter l'accès aux agents des relations de travail.
4 Achat d'une serrure de porte à clavier et de quatre avertisseurs individuels.
5 Achat d'un pupitre, d'une chaise, d'un téléphone et autre matériel de bureau pour le gardien de sécurité.
6 Achat de deux avertisseurs individuels et des matériaux nécessaires à la construction de deux salles d'entrevue sécurisées.
7 Installation de la serrure de porte à clavier.
8 Installation de la serrure de porte à clavier et des quatre avertisseurs individuels.
9 Branchement du téléphone et déménagement de l'ameublement.
10 Construction de deux salles d'entrevue sécurisées et installation de deux avertisseurs individuels.
11 Salaire d'un analyste de la sécurité pour documenter les procédures de contrôle d'accès et d'intervention d'urgence.
12 Salaire d'un analyste de la sécurité pour documenter les procédures de contrôle d'accès et d'intervention d'urgence.
13 Salaire d'un analyste de la sécurité pour documenter les procédures de contrôle d'accès et d'intervention d'urgence.
14 Salaire d'un analyste de la sécurité pour documenter les procédures d'intervention d'urgence.
15 Salaires d'un analyste de la sécurité et des agents des relations de travail pour la formation initiale à l'équipement et aux procédures.
16 Coûts annuels de formation des nouveaux employés, en présumant un roulement complet du personnel tous les quatre ans.
17 Salaires d'un analyste de la sécurité et des agents des relations de travail pour la formation initiale à l'équipement et aux procédures.
18 Coûts annuels de formation des nouveaux employés, en présumant un roulement complet du personnel tous les quatre ans.
19 Salaires d'un analyste de la sécurité et des gardiens de sécurité pour la formation initiale aux procédures d'intervention d'urgence.
20 Coûts annuels de formation des nouveaux gardiens de sécurité, en présumant un roulement complet du personnel tous les deux ans.
21 Salaires d'un analyste de la sécurité et des agents des relations de travail pour la formation initiale aux procédures d'intervention d'urgence.
22 Coûts annuels de formation des nouveaux employés, en présumant un roulement complet du personnel tous les quatre ans.
23 En présumant de l'existence actuelle d'un poste central de garde dans l'immeuble, il n'y a pas coût salarial supplémentaire pour qu'un des gardiens puisse répondre aux alarmes.

Coûts	Option 1	Option 2	Option 3	Option 4
Entretien	100 $[25]	200 $[26]	–	300 $[27]
Productivité réduite	–[28]	–[29]	2 800 $[30]	–
Efficacité accrue	–	–	–[31]	–[32]
Total des coûts ponctuels	1 450 $[33]	3 150 $[34]	1 400 $[35]	32 000 $[36]
Coûts annuels récurrents	200 $[37]	325 $[38]	40 400 $[39]	325 $[40]

Tableau F4-1 : Coûts initiaux et récurrents directs et indirects

4.3 Rentabilité des mesures de protection

La rentabilité relative de chaque option est calculée en trois étapes, comme suit :

- **Coût annuel amortis.** Alors que l'on peut s'attendre que les éléments durables, telles les salles d'entrevue sécurisées, subsistent presque indéfiniment, les changements organisationnels se produisent plus fréquemment; il semble donc plus réaliste, voire même légèrement optimiste, de choisir une durée de vie de dix ans pour chacune des options pour calculer les coûts annuels amortis dans le tableau F4-2. Il convient de noter, au fur et à mesure que s'accroît la durée de vie projetée des mesures de protection, que le coût annuel amorti de l'option 4 diminue de manière significative puisqu'elle requiert beaucoup de capitaux en raison de dépenses initiales plus élevées. D'autre part, le coût

24 Montant basé sur un salaire horaire de 15 $ pour la présence d'un gardien de sécurité de 7 h 30 à 17 h 30 chaque jour ouvrable.
25 Vérification annuelle d'entretien de la serrure de porte à clavier.
26 Vérification annuelle d'entretien de la serrure de porte à clavier et des avertisseurs individuels.
27 Vérification annuelle d'entretien des salles d'entrevue sécurisées et des avertisseurs individuels.
28 Le besoin d'accompagner les visiteurs aura une incidence négative sur la productivité; toutefois, cette lacune sera probablement compensée par une amélioration du moral due à un meilleur sentiment de sécurité.
29 Encore une fois, le besoin d'accompagner les visiteurs aura une incidence négative sur la productivité; toutefois, cette lacune sera probablement compensée par une amélioration du moral due à un meilleur sentiment de sécurité.
30 L'imposition d'une politique en matière de rangement du bureau et l'utilisation de numéros séquentiels augmenteront légèrement (d'environ un pour cent) la charge de travail des agents des relations de travail.
31 Malgré une augmentation possible de la productivité due à un meilleur moral et à une plus grande sensibilisation à la sécurité, les avantages réels sont difficiles à prévoir.
32 Malgré une augmentation possible de la productivité due à un meilleur moral et à une plus grande sensibilisation à la sécurité, les avantages réels sont difficiles à prévoir.
33 Coûts de l'acquisition, de l'installation, de la documentation et de la formation initiale.
34 Coûts de l'acquisition, de l'installation, de la documentation et de la formation initiale.
35 Coûts de l'acquisition, de l'installation, de la documentation et de la formation initiale.
36 Coûts de la conception, du développement, de l'acquisition, de l'installation, de la documentation et de la formation initiale.
37 Vérifications annuelles d'entretien et coûts de la formation des nouveaux employés.
38 Vérifications annuelles d'entretien et coûts de la formation des nouveaux employés.
39 Salaire et avantages du gardien de sécurité, coûts annuels de formation des nouveaux employés et perte de productivité due à l'imposition d'une politique en matière de rangement du bureau et à l'utilisation de numéros séquentiels.
40 Vérifications annuelles d'entretien et coûts de la formation des nouveaux employés.

total de possession de l'option 3 continue de croître constamment en raison des salaires annuels permanents.

- **Réduction totale des risques.** On peut calculer très facilement la réduction totale des risques de chaque option en comparant les risques résiduels projetés des tableaux F3-4 à F3-6 de l'appendice F-3 aux risques résiduels évalués initiaux du tableau F3-2. La diminution est ensuite reportée dans le tableau F4-2 ci-dessous.
- **Rentabilité des mesures de protection.** La rentabilité relative mesurée de chaque option représente la dépense annuelle pour chaque niveau de réduction de risques indiqué sur la dernière rangée du tableau F4-2.

Rentabilité	Option 1	Option 2	Option 3	Option 4
Durée utile prévue	10 ans	10 ans	10 ans	10 ans
Coût annuel amorti	345 $	640 $	40 540 $	3 525 $
Réduction totale du risque	8/11[41]	11	10	10
Rentabilité	43,13 $/31,36 $	58,18 $	4 054 $	352,50 $

Tableau F4-2 : Calcul de la rentabilité des mesures de protection

4.4 Conclusion

Bien que l'option 1 offre une solution plus rentable que les autres, un certain doute persiste quant à son efficacité au plan des menaces de harcèlement et d'agression puisque les employés peuvent être réticents à intervenir. Si une telle situation devait se produire, cette option ne permettrait pas d'atteindre le risque résiduel cible, c.-à-d., un niveau moyen. La prudence impose donc de retenir l'option 2, qui n'est que marginalement moins rentable mais permet d'obtenir la réduction requise des risques. Les options 3 et 4 permettent également d'atteindre des résultats acceptables, mais à des coûts beaucoup plus élevés pour chaque niveau de réduction de risques. Lors de la production du rapport d'EMR final, les données saisies dans l'option 2 ci-dessus doivent être transférées dans le tableau des recommandations illustré à l'appendice F-5.

Nota :

Les coûts présentés dans cet exemple ne sont pas nécessairement complets ni définitifs. Nous les proposons à titre d'exemple pour illustrer le calcul de la rentabilité à l'appui des recommandations finales d'un rapport d'EMR.

[41] Le chiffre le plus faible (8) représente une évaluation plus prudente de la situation où les autres employés peuvent être réticents à intervenir en cas de harcèlement ou d'agression, et le deuxième chiffre (11) reflète une plus forte réduction du risque dans le cas où les employés témoignent d'une capacité d'intervention efficace.

Page intentionnellement laissée en blanc

Appendice F-5 – Tableau des recommandations

Recommandation n^{o} 1 :													
Coûts connexes													
Coûts directs						**Avantages/coûts indirects**		**Coût total de possession**					
Conception	**Acquisition**	**Installation**	**Activités courantes**		**Autre**	**Productivité réduite**	**Efficacité accrue**						
Durée utile prévue	**Coût annuel amorti**	**Interdépendance des mesures de protection**	**1.**										
			2.										
			3.										
Risques résiduels évalués inacceptables								**Risques résiduels projetés**					
Bien	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	**R**		**Bien**	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	**R**
Rentabilité des mesures de protection														
Réduction totale des risques (niveaux)								**Rentabilité ($/niveau)**						
Autres considérations														

1 Instructions

Le formulaire *Tableau des recommandations* est un outil commode pour faire état de l'analyse sur laquelle repose chaque proposition visant à réduire à un niveau acceptable les risques résiduels inacceptables. L'information pertinente doit y être entrée comme suit :

- **Étape 1.** Remplissez un formulaire distinct pour chaque recommandation et numérotez les recommandations par ordre séquentiel, en commençant par la plus rentable et en terminant par la moins rentable. Faites une brève description dans la première cellule du tableau, par exemple : « Installer un système d'alarme anti-intrusion avec capteurs magnétiques sur toutes les portes et les fenêtres, et des détecteurs de mouvement à infrarouge et des détecteur de bris de vitre dans chaque pièce ».
- **Étape 2.** Détaillez tous les coûts directs et indirects connexes et calculez le coût total de possession, conformément aux sections 4.2 et 4.3 de l'annexe F.
- **Étape 3.** Évaluez la durée utile prévue (en années) de la mesure de protection proposée.
  Étape 4. Calculez le coût annuel amorti de la mesure de protection recommandée, conformément à la section 4.4.2 de l'annexe F. **Nota :** Si vous déterminez des interdépendances à l'étape 5 et que la mise en œuvre et l'exploitation de la ou des mesures de protection recommandées doivent entraîner des coûts, vous devez additionner le coût annuel amorti de toutes les mesures interdépendantes pour calculer leur rentabilité globale (étape 9).
- **Étape 5.** Énumérez toutes les interdépendances avec d'autres mesures de protection existantes ou proposées, conformément à la section 3.3.8 de l'annexe F. Cette étape est particulièrement importante, car l'efficacité d'une recommandation peut dépendre de la mise en œuvre d'une autre mesure de sécurité connexe. Si elles ne sont pas approuvées, le risque résiduel résultant ne sera peut-être pas acceptable. Pour revenir à notre exemple du système d'alarme anti-intrusion, la présence d'une force d'intervention (gardes de sécurité ou service de police local) serait une interdépendance essentielle.
- **Étape 6.** Reprenez de la liste des risques résiduels de l'appendice E-2 toutes les combinaisons de risques inacceptables que la mesure de protection recommandée viserait.
- **Étape 7.** Entrez la nouvelle valeur des biens ou les nouveaux niveaux de menace et de vulnérabilité à la suite de la mise en œuvre de la mesure de protection recommandée et calculez le risque résiduel prévu conformément à la section 5 de l'annexe F.
- **Étape 8.** Comparez les niveaux de risque résiduel évalués et projetés pour chaque entrée et calculez leur réduction totale conformément à la section 4.4.3 de l'annexe F.
- **Étape 9.** Calculez le rapport coût-efficacité relatif de la mesure de protection recommandée conformément à la section 4.4.4 de l'annexe F.
- **Étape 10.** Notez toute autre considération, comme la disponibilité de la mesure proposée, son acceptabilité, les besoins en matière de formation et la conformité de la mesure aux normes obligatoires ou aux pratique exemplaire reconnues.

2 Exemple

Si l'installation d'un système d'alarme anti-intrusion est proposée pour protéger contre le vol et contre l'espionnage industriel, respectivement, les obligations au porteur et les dossiers financiers sensibles conservés dans un dépôt gouvernemental, le tableau des recommandations pourrait se présenter ainsi :

Recommandation n^{o} 1 :
Installer un système d'alarme anti-intrusion avec capteurs magnétiques sur toutes les portes et les fenêtres du dépôt central des dossiers. Installer des détecteurs de mouvement à infrarouge et des détecteurs de bris de vitre dans les pièces D-101 et D-103.

Coûts connexes							
Coûts directs					**Avantages/coûts indirects**		**Coût total de possession**
Conception	**Acquisition**	**Installation**	**Activités courantes**	**Autre**	**Productivité réduite**	**Efficacité accrue**	
-	2 000 $	1 500 $	750 $/année[1]	250 $[2]			

Durée utile prévue	**Coût annuel amorti**	**Interdépendance des mesures de protection**
10 ans[6]	1 125 $[7]	1. Les murs du dépôt sont déjà solidement construits.[3] 2. Il est recommandé que les portes soient renforcées et que des barreaux soient posés aux fenêtres.[4] 3. Les obligations au porteur et les documents sensibles sont entreposés dans des coffres-forts.[5] 4. Le service de police local peut intervenir dans un délai de 10 minutes ou moins.[8]

1 En supposant des frais de surveillance de 60 $ par mois et une inspection annuelle de 150 $.

2 Coûts de la formation ponctuelle de dix employés.

3 Cette mesure connexe est une mesure de prévention destinée à ralentir une intrusion. Elle est déjà en place, de sorte qu'il n'y aurait pas de dépenses supplémentaires qui se répercuteraient sur le coût annuel amorti de la recommandation.

4 Les portes et fenêtres ne sont pas renforcées pour l'instant, de sorte qu'un intrus déterminé pourrait s'introduire par effraction et mettre la main sur les obligations au porteur ou les documents sensibles en quelques minutes. Dans ce cas, le coût supplémentaire de 4 000 $ de la mise en place de ces mesures préventives doit être inclus dans le calcul final de la rentabilité.

5 On peut s'attendre à ce que les coffres-forts, qui représentent une autre mesure de prévention, retardent l'accès non autorisé d'environ 15 minutes après l'entrée non autorisée. Il n'y aurait pas non plus de dépenses supplémentaires, les coffres-forts sont déjà là.

6 Même si un système d'alarme est censé durer plus de dix ans, on tient pour acquis que le dépôt sera vraisemblablement réorganisé ou déménagé au moins tous les dix ans, ce qui nécessitera l'installation d'un nouveau système. Des hypothèses de ce genre peuvent être indiquées dans la section Autres considérations.

7 Calcul : coûts de l'acquisition et de l'installation et autres coûts plus dix fois les frais annuels d'exploitation, divisés par la durée utile prévue, soit 2 000 $ + 1 500 $ + 250 $ = 3 750 $ + (10 × 750 $) ÷ 10 = 1 125 $.

8 Le service de police local intervient en cas de besoin, car autrement, l'installation d'un système d'alarme anti-intrusion, qui est un mécanisme de détection, ne servirait à rien.

Risques résiduels évalués inacceptables							Risques résiduels projetés						
Bien	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	**R**	**Bien**	**B_{Val}**	**Menace**	**M**	**Vulnérabilité**	**V**	**R**
obligations	E	vol	E	accessibilité absence de système de détection	E	E	obligations	E	vol	E	accessibilité absence de système de détection	F	M
documents sensibles	M	espionnage industriel	E	accessibilité absence de système de détection	E	E	documents sensibles	M	espionnage industriel	E	accessibilité absence de système de détection	F	M
Rentabilité des mesures de protection													
Réduction totale du risque (niveaux)				4			**Rentabilité ($/niveau)**				381 $[9]		
Autres considérations													
1. Même si un système d'alarme est censé durer plus de dix ans, on tient pour acquis que le dépôt sera vraisemblablement réorganisé ou déménagé au moins tous les dix ans, ce qui nécessitera l'installation d'un nouveau système.													

[9] Coût annuel amorti initial de 1 125 $ rajusté de 400 $ pour tenir compte du coût du renforcement des portes et des fenêtres, divisé par la réduction des risques (de quatre niveaux).

Appendice F-6 – Plan du rapport d'EMR

Plan du rapport d'EMR	Renvois
Résumé • Recommandé pour tous les rapports, sauf les plus courts. • Présenté sur une ou deux pages pour décrire : o le but et l'objet de l'évaluation; o les risques résiduels évalués inacceptables; o les principales recommandations; o le coût estimatif de toutes les recommandations; et o le risque résiduel projeté une fois que les recommandations ont été approuvées et mises en œuvre.	
Contexte • Identifier l'organisation ou le ministère. • Fournir un contexte pour le projet d'EMR et décrire : o le secteur d'activité et son environnement opérationnel; o les niveaux de prestation de services et les obligations; o la justification d'une nouvelle installation ou d'un nouveau système de TI; ou o le problème de sécurité particulier à traiter. • Le contenu réel varie selon l'objet et le but de l'évaluation.	Appendice A-6, Section 1, Contexte.
But • Énoncer l'objectif du projet d'EMR en une seule phrase.	Annexe A, Section 4.2.1, Objet de l'évaluation.
Mandat • Résumer brièvement les pouvoirs de l'équipe d'EMR. • Joindre une copie des instructions écrites. • Joindre une copie du plan de travail approuvé de l'EMR.	Annexe A, Section 3, Mandat du projet d'EMR. Appendice A-6, Exemple de plan de travail de l'EMR.
Portée • Identifier l'objet du projet d'EMR. • Définir les limites de l'évaluation et indiquer : o ce qui est inclus dans la portée de l'évaluation du projet d'EMR; et o les biens connexes qui ne le sont pas.	Annexe A, Section 4, Portée de l'évaluation.

Plan du rapport d'EMR	Renvois
• Utiliser les diagrammes schématiques ou les plans d'étage pour illustrer la portée. • Noter les rapports d'EMR connexes : o décrire leurs relations par rapport à l'évaluation actuelle; et o en produire la liste dans une pièce jointe.	
Identification et évaluation des biens • Décrire : o les biens corporels et incorporels les plus importants, normalement au niveau du groupe ou du sous-groupe; o les employés qui comptent sur ces biens pour s'acquitter de leurs tâches; o les services qu'offrent les biens; et o les préjudices potentiels advenant une compromission. • Un court paragraphe suffit généralement pour chaque entrée. • Résumer les autres éléments dans le tableau d'évaluation des biens/énoncé de sensibilité, qui doit être joint en annexe.	Annexe B, Phase d'identification et d'évaluation des biens. Appendice B-5, Tableau d'évaluation des biens.
Évaluation des menaces • Décrire les menaces les plus graves, normalement au niveau de détail de la catégorie d'activité ou d'agent. • Indiquer les biens menacés et les types probables de compromission. • Un court paragraphe suffit généralement pour chaque entrée. • Résumer les autres éléments dans le tableau d'évaluation des menaces, qui doit être joint en annexe.	Annexe C, Phase d'évaluation des menaces. Appendice C-4, Tableau d'évaluation des menaces.
Évaluation des vulnérabilités • Décrire les vulnérabilités graves, normalement au niveau du groupe. • Indiquer les biens visés et les menaces favorisées. • Éviter d'inclure un trop grand nombre de détails techniques dans le corps du rapport. • Un court paragraphe suffit généralement pour chaque entrée. • Résumer les autres éléments dans le tableau d'évaluation des vulnérabilités, qui doit être joint en annexe.	Annexe D, Évaluation des vulnérabilités. Appendice D-4, Tableau d'évaluation des vulnérabilités.
Évaluation des risques • Décrire tous les risques résiduels évalués inacceptables. • Pour simplifier l'évaluation : o mettre l'accent sur les risques les plus graves; et o consolider le plus de risques possibles en groupes généraux. • Un court paragraphe suffit généralement pour chaque entrée.	Annexe E, Calcul des risques résiduels.

Plan du rapport d'EMR	Renvois
• Résumer les autres éléments dans la liste des risques résiduels évalués, qui doit être jointe en annexe.	Appendice E-2, Liste des risques résiduels évalués.
Recommandations • Résumer chacune des recommandations, y compris leurs coûts. • Présenter le risque résiduel projeté. • Saisir les détails dans une annexe.	 Annexe F, Phase des recommandations. Appendice F-5.
Pièces jointes • Certains des éléments ci-dessous peuvent ne pas s'appliquer à chaque cas : o Mandat du projet d'EMR (là où il est énoncé clairement). o Plan de travail de l'EMR (incluant la liste de tous les membres de l'équipe de l'EMR). o Rapports d'EMR connexes (le cas échéant). o Tableau d'évaluation des biens/énoncé de sensibilité. o Tableau d'évaluation des menaces. o Tableau d'évaluation des vulnérabilités. o Liste des risques résiduels évalués. o Tableau des recommandations. o Personnel interviewé et sites visités. o Documents de référence, incluant : ▪ Lois fédérales pertinentes, ▪ Politiques et directives gouvernementales et ministérielles, ▪ Normes et lignes directrices en matière de sécurité, ▪ Documentation de conception, ▪ Plans des sites, ▪ Manuels d'utilisation et d'exploitation du fournisseur, ▪ Rapports d'incidents/Évaluations des menaces, ▪ Rapports d'évaluation des produits, ▪ Évaluation des vulnérabilités, ▪ Test de sécurité et rapports d'évaluation.	 Appendice A-6. Appendice B-5. Appendice C-4. Appendice D-4. Appendice E-2. Appendice F-5

Page intentionnellement laissée en blanc

Appendice F-7 – Exemple de rapport d'EMR

1 Contexte

La Division des affaires internes (DAI) de la Direction générale des services ministériels effectue des enquêtes préliminaires concernant les allégations de fraude, d'espionnage industriel et autres infractions contre les biens ministériels afin de déterminer les motifs qui justifieraient la tenue d'une enquête criminelle par la police locale. Compte tenu du caractère sensible de situations particulières, certains dossiers sont cotés Protégé C. La section 16.4.9 de la Norme opérationnelle de sécurité –Gestion de la sécurité des technologies de l'information (GSTI) stipule ce qui suit : « Au Canada, les ministères devraient appliquer la norme TEMPEST à l'information très secrète et aux renseignements protégés C lorsqu'une évaluation des menaces et des risques le justifie. »

2 But

Le but de ce projet d'EMR est de déterminer si le réseau local de la DAI requiert une protection TEMPEST.

3 Mandat

Le plan de travail de l'EMR, à l'annexe A, indique que l'équipe d'EMR, formée de représentants de la DAI, de la Direction du dirigeant principal de l'information et du coordonnateur de la sécurité des TI, est chargée d'évaluer les risques de sécurité liés aux émissions et de recommander une des quatre options prévues à la section 3.3 de l'ITSG-12, *Procédures d'évaluation des installations du gouvernement du Canada*.

4 Portée

La DAI, au 3^{e} étage de l'édifice de l'administration centrale, doit être dotée d'un réseau local autonome comprenant dix postes de travail et un serveur individuel pour le traitement de l'information classifiée et protégée. Toutes les mesures de sécurité matérielle, du personnel et des TI recommandées dans le Rapport d'EMR 41/05 ont été ou seront mises en œuvre et testées; donc, à l'exception des aspects concernant la protection TEMPEST, le système est prêt pour les activités finales de certification et d'accréditation.

5 Identification et évaluation des biens

La DAI effectue environ 150 enquêtes par année. La plupart des rapports sont cotés Protégé B, mais un petit nombre d'entre eux qui concernent l'espionnage industriel sont classifiés Secret. Environ 20 % des dossiers sont cotés protégé C puisqu'il existe un risque raisonnable que toute divulgation non autorisée puisse mettre en danger la vie de sources confidentielles et

compromettre les poursuites judiciaires intentées contre les groupes criminels organisés responsables d'actes frauduleux dont la valeur est souvent supérieure à 10 millions de dollars. Par conséquent, on attribue aux ressources d'information prévues dans la portée de cette évaluation la valeur **Élevé**.

6 Évaluation des menaces

Au cours de la dernière année, des gangs du crime organisé ont tenté, à au moins trois occasions, de corrompre des employés du ministère pour avoir accès à des dossiers de la DAI. On attribue donc à la probabilité d'une occurrence future la cote **Élevé**. Même si ces groupes criminalisés possèdent d'importantes ressources financières, ils n'ont pas démontré qu'ils avaient les connaissances et les compétences requises pour mener une attaque TEMPEST. On attribue donc à la gravité de la menace criminelle la cote **Moyen**. Néanmoins, malgré la probabilité de niveau **Élevé** et la gravité de niveau **Moyen**, le niveau global de la menace demeure **Élevé**.

7 Évaluation des vulnérabilités

7.1 Mesures de protection existantes

Tel que l'indique la Figure F7-1, l'édifice de l'administration centrale se trouve en plein champ dans un espace visible et contrôlé sur une distance de presque 200 m. Tous les visiteurs s'identifient à l'entrée principale et sont accompagnés partout où ils circulent dans les installations. Une patrouille surveille régulièrement le terrain de stationnement pour déceler et signaler la présence de tout véhicule non autorisé. Le transformateur de l'édifice se trouve dans un local verrouillé au sous-sol. Aucun dispositif sans fil n'est permis dans les installations. Le serveur de la DAI se trouve dans une salle verrouillée dotée de contrôles d'accès évolués. Tout le câblage de connexion au réseau local, incluant les liens de fibre optique, est protégé dans des armoires de télécommunications verrouillées.

7.2 Vulnérabilités connexes

La combinaison de l'espace visible, des critères d'installation et des contrôles d'accès rigoureux offre des mesures de protection efficaces qui empêchent toute attaque TEMPEST; d'autre part, les patrouilles motorisées effectuées par les gardiens de sécurité offrent un mécanisme de détection modérément efficace. On attribue donc à la vulnérabilité globale de l'administration centrale la cote **Faible**, fondée sur une incidence **Faible** de la probabilité de compromission et une incidence de la gravité des résultats de niveau **Moyen**.

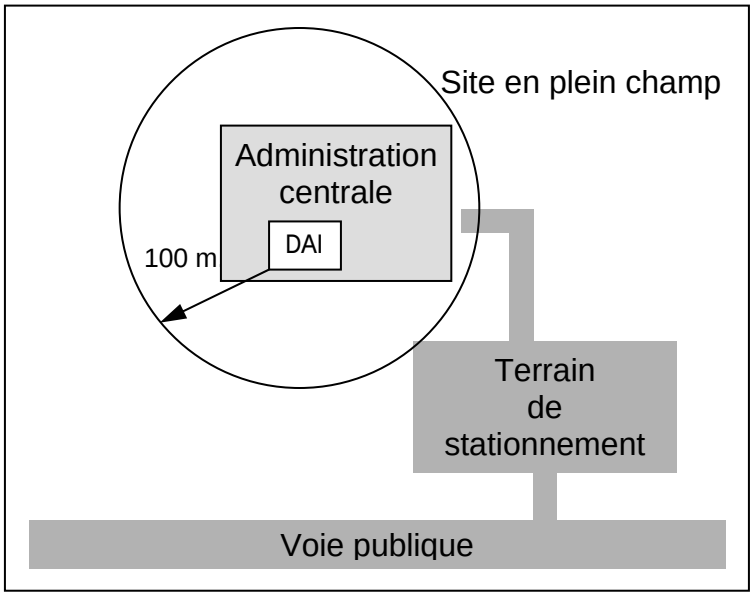

Figure F7-1: Plan du site de l'administration centrale

8 Évaluation des risques

Le niveau **Élevé** des valeurs des biens, le niveau **Élevé** de la menace et le niveau **Faible** des vulnérabilités font en sorte que le risque résiduel évalué est coté **Moyen**, niveau généralement acceptable, tel qu'indiqué dans le tableau 1.

Bien (Groupe/Sous-gr.)	Valeurs des biens			Menace connexe (Catégorie d'activité/agent)	M	Vulnérabilités connexes	V	Risque résiduel ($B_{Val} \times T \times V$)	R
	C	D	I						
Dossiers d'enquête de la DAI	E	–	–	Groupes criminels organisés	E	Voir la narration	F	$4 \times 4 \times 2 = 32$	M

Tableau F7-1 : Calcul du risque résiduel évalué

9 Recommandations

Dans les circonstances, il n'y a pas lieu d'encourir des coûts supplémentaires de 300 % pour l'acquisition d'un équipement TEMPEST de Niveau 1, tel que défini dans l'ITSG-12, *Procédures d'évalution des installations du gouvernement du Canada*. Même avec des postes de travail et des serveurs disponibles sur le marché, le niveau du risque résiduel évalué se situe dans la gamme acceptable de niveau **Moyen**. On recommande donc l'achat, chez un fournisseur certifié ISO 9000, d'équipement de niveau 3, essentiellement des postes de travail et des serveurs disponibles sur le marché, et leur installation dans le réseau local de la DAI. Pour empêcher toute détérioration de la posture de sécurité actuelle, on recommande également :

- que l'agent de sécurité des installations examine tous les mois les procédures de contrôle d'accès de l'édifice et les registres des visiteurs pour y déceler toute anomalie indiquant des activités de menace potentielles;
- que l'administrateur de système inspecte le réseau local de la DAI tous les six mois pour déceler tout signe de trafiquage ou de modifications non autorisées; et
- que la cellule de sensibilisation à la sécurité fournisse aux gardiens motorisés de la formation supplémentaire et des breffages de renforcement réguliers pour identifier et signaler toute menace d'attaque TEMPEST potentielles.

10 Pièces jointes

- Plan de travail de l'EMR.
- Rapport d'EMR 41/05, Bureaux et réseau local de la DAI.
- Liste des références.

Nota :

1. Le but de cet exemple de rapport d'EMR est d'illustrer l'évaluation ciblée d'un problème très spécifique, soit le besoin de protection TEMPEST pour un réseau local chargé du traitement de l'information cotée Protégé C au Canada.
2. Il n'est pas vraiment nécessaire de préparer de résumé pour un rapport d'EMR de cette taille.
3. Pour éviter d'utiliser de l'information classifiée ou protégée dans cet exemple, certaines des références à l'ITSG-12, *Procédures d'évaluation des installations du gouvernement du Canada*, ont été simplifiées ou énoncées de manière indirecte.
4. Cet exemple de rapport d'EMR ne devrait pas être appliqué directement à une évaluation réelle sans examen plus poussé.

Annexe G - Conclusion

1 Introduction

1.1 Généralités

Les cinq phases d'un projet d'EMR, qui comptent en tout 21 processus séquentiels et six résultats successifs, sont décrites brièvement dans le sommaire de gestion, et considérablement développées aux annexes A à F; d'autres détails sont également exposés dans un certain nombre d'appendices. Bien que la présente documentation donne la méthodologie complète d'EMR, la conclusion propose du matériel d'appui qui s'ajoute aux outils de base et rehausse leur utilité :

- **Processus connexes.** Le rapport d'EMR constitue un intrant important pour les guides de sécurité du site et de la conception portant sur la sécurité matérielle, ainsi que pour la certification et l'accréditation des systèmes de TI.
- **Pratiques exemplaires d'EMR.** Conseils pratiques visant à accélérer le processus d'EMR et à atteindre des résultats davantage cohérents.
- **Feuille de travail EMR.** Simple feuille de travail constituant un aide-mémoire utile pour les spécialistes de la sécurité menant un projet d'EMR.
- **Sensibilité des rapports d'EMR.** Explication de certains facteurs à prendre en considération pour attribuer une cote Classifié ou Protégé aux rapports d'EMR.
- **Glossaire et acronymes.** Liste complète de tous les termes et abréviations utilisés dans la *Méthodologie harmonisée d'EMR*, dressée afin d'améliorer les communications et de favoriser l'interopérabilité entre les projets d'EMR interdépendants.
- **Références.** Liste de tous les documents cités dans le corps du texte, classés en ordre alphabétique, par catégorie; les sources sont précisées dans la mesure du possible afin de faciliter la consultation.

1.2 But

Le but de la présente annexe est de faire connaître divers documents à l'appui de la méthodologie harmonisée d'EMR décrite dans le corps du document, ainsi que de promouvoir une mise en application uniforme de la méthodologie dans le cadre de divers projets d'EMR.

2 Processus connexes

2.1 Généralités

Comme il est expliqué à la section 7.2 du sommaire de gestion et encore à l'appendice A-2, portant sur les normes de sécurité et les évaluations des menaces et des risques, l'EMR est un élément important d'un programme de gestion permanente des risques, mais ne constitue pas à elle seule une solution complète. De fait, un rapport d'EMR doit être examiné de concert avec

d'autres processus connexes pour permettre l'atteinte de résultats exhaustifs. Ces processus interdépendants comprennent des énoncés de sécurité matérielle pour la sélection et la conception de nouvelles installations, la certification et l'accréditation de systèmes de TI, la gestion des configurations et le contrôle des changements (pour déterminer si l'évaluation doit être mise à jour au fil de l'évolution des installations et des systèmes de TI), ainsi que des mécanismes de réaction aux incidents qui identifient les nouvelles menaces ou vulnérabilités.

2.2 Guides de sécurité du site et de la conception

Un guide de sécurité du site doit être préparé chaque fois qu'un nouvel emplacement est choisi pour la location, l'achat ou la construction de nouvelles installations. Le rapport d'EMR à l'appui doit alors préciser les problèmes de sécurité propres au site (menaces et vulnérabilités), par exemple le haut taux de vandalisme, de vols ou de crimes violents dans le quartier, ou les risques élevés d'inondation et autres sinistres naturels. Lorsque l'emplacement est sélectionné, un guide de sécurité de la conception doit être préparé pour recommander les mesures de protection appropriées à la fois pour les structures déjà en place et les nouvelles constructions. Encore une fois, le rapport d'EMR à l'appui doit confirmer les valeurs des biens des installations et, renseignement encore plus important, le personnel et les services offerts depuis le site, ainsi que toute menace susceptible d'avoir des répercussions défavorables sur les biens, et les vulnérabilités connexes qui pourraient exposer les biens à des préjudices. Bien que les mesures de protection recommandées soient déterminées par une analyse de ces données dans le rapport d'EMR, elles sont généralement omises ou brièvement résumées dans le guide de sécurité de la conception subséquent afin d'éviter d'avoir à attribuer au document une cote de sécurité Classifié ou Protégé supérieure.[1]

Guide de sécurité du site
Document décrivant les attributs de *sécurité matérielle* recherchés dans un site lorsque les installations sont déménagées.

1.1.1.1 Guide de sécurité de la conception
Document décrivant la philosophie et les principes de protection matérielle des installations, ainsi que les mesures de protection matérielle.

Guide de sécurité SST/GS-25
Guide pour la préparation d'un énoncé de sécurité matérielle, janvier 2000

2.3 Certification et accréditation (C et A)

En vertu de la section 10.12.1(a) de la PGS, les ministères sont tenus de certifier et d'accréditer les systèmes de TI avant que ceux-ci ne soit mis en production. Comme le précise la définition, le processus de certification comprend un examen

Certification *(certification)* – Évaluation complète des dispositifs de sécurité techniques et non techniques d'un système des TI et d'autres mesures de sauvegarde connexes, effectuée à l'appui de l'accréditation, pour déterminer le degré selon lequel un modèle de conception et de mise en œuvre précis satisfait à un ensemble donné d'exigences en matière de sécurité.

Accréditation *(accreditation)* – Autorisation officielle par la direction d'exploiter un système des TI et acceptation par la direction du risque résiduel s'y rattachant. L'accréditation dépend des résultats de la certification ainsi que d'autres considérations de nature administrative.

Politique du gouvernement sur la sécurité, février 2002

[1] Pour obtenir des directives détaillées sur les guides de sécurité du site et de la conception, consultez le Guide de sécurité de la GRC SST/GS-25, *Guide pour la préparation d'un énoncé de sécurité matérielle*.

rigoureux de toutes les mesures de protection associées à un système de TI afin de répondre à deux questions de base, à savoir : (1) Des mesures de sécurité appropriées ont-elles été prises pour satisfaire à la politique de sécurité du système? (2) Ces mesures ont-elles été mises en œuvre correctement? En résumé, la certification vise à recueillir suffisamment de preuves pour donner à l'accréditeur l'assurance que le système est assez sûr pour répondre aux exigences et aux besoins opérationnels. À cet égard, le rapport final d'EMR est probablement l'élément le plus important pour la prise d'une décision finale à propos de la certification, puisqu'il rend compte d'une évaluation objective des biens, de leurs valeurs, des menaces et des vulnérabilités connexes, ainsi que de l'incidence des mesures de protection recommandées sur les risques résiduels du projet.[2]

2.4 Gestion des configurations et contrôle des changements

Il n'existe pas d'installations ni de système de TI qui demeurent statiques au fil du temps. Des modifications sont souvent apportées et de nouveaux biens assortis de différentes valeurs sont introduits avant même que l'objet du rapport initial d'EMR soit entièrement déployé et complètement opérationnel. Il va de soi que tout changement à la conception initiale des installations ou d'un système de TI est susceptible d'introduire des risques nouveaux et éventuellement inacceptables. C'est pourquoi les sections 10.11 et 10.12.1(b) de la PGS obligent les ministères à examiner en permanence les mesures de sécurité matérielle et à mener régulièrement une évaluation des changements à la configuration des TI, de manière à déterminer toutes les incidences sur les risques résiduels. Comme bon nombre de modifications ne touchent qu'un petit sous-ensemble des biens identifiés dans le rapport initial d'EMR, les révisions nécessaires pour évaluer les répercussions sur la sécurité des modifications ou des ajouts proposés peuvent se faire assez rapidement pour appuyer une prise de décision éclairée, pourvu que l'EMR, la gestion des configurations et les processus de contrôle des changements du ministère soient étroitement liés. En règle générale, aucun changement ne devrait être approuvé tant que le rapport d'EMR n'a pas été mis à jour et que des mesures de protection satisfaisantes n'ont pas été cernées, le cas échéant, pour traiter les risques inacceptables découlant des modifications. L'inscription de la date et du numéro de version sur les rapports d'EMR facilite le suivi des changements.

2.5 Mécanismes de réaction aux incidents

Dans le même ordre d'idées, de nouvelles menaces et vulnérabilités se manifestent régulièrement. Certaines peuvent être repérées de manière proactive grâce à un suivi permanent des publications professionnelles, des médias et des rapports de renseignement, alors que d'autres sont décelées après le fait accompli, alors qu'on réagit à des incidents de sécurité. Dans les deux cas, les rapports d'EMR existants doivent être mis à jour pour tenir compte des nouvelles évaluations des menaces et vulnérabilités, et les risques résiduels devraient être calculés à nouveau. Lorsque les nouveaux risques dépassent le seuil acceptable, des mesures correctives doivent être recommandées afin de maintenir une position satisfaisante en matière de

[2] Pour obtenir des directives détaillées sur la certification et l'accréditation, consultez la publication MG-4 du CST, *Guide de certification et d'accréditation des technologies de l'information*.

sécurité. Encore une fois, la réutilisation des rapports d'EMR existants permet d'accélérer la réaction à tout nouveau facteur.

3 Pratiques exemplaires d'EMR

Comme il en est question dans l'introduction,[3] les objectifs de la méthodologie harmonisée d'EMR comprennent une simplicité intuitive, une modularité améliorée et une souplesse accrue afin d'améliorer à la fois la cohérence et l'interopérabilité. Certaines lignes directrices ou pratiques exemplaires de base permettant d'atteindre des résultats optimaux grâce à la nouvelle méthodologie ont été extraites de chacune des annexes et sont résumées ci-dessous.

- Restreindre le plus possible la portée de chaque projet d'EMR.
- Décomposer les installations, les systèmes ou les activités opérationnelles en modules afin de permettre la production de plusieurs rapports d'EMR d'envergure moindre, plutôt que d'un seul rapport atteignant des proportions écrasantes.
- Définir tous les liens entre les rapports d'EMR connexes.
- Consigner toutes les variables de risque pertinentes incluses dans la portée de l'évaluation de manière résumée, tout en se concentrant sur les biens de plus grande valeur, les menaces les plus importantes et les vulnérabilités les plus graves, c'est-à-dire celles qui sont le plus susceptibles d'entraîner des risques résiduels inacceptables.
- Ne pas suranalyser les variables de risque. La première évaluation intuitive des valeurs des biens, des menaces et des vulnérabilités est généralement plus précise et toujours plus efficace que des arguments complexes portant sur des possibilités obscures.
- Dans le même ordre d'idée, il convient d'éviter les scénarios de menace complexes pour se concentrer principalement sur les menaces directes.
- Si des membres de l'équipe de l'EMR ne s'entendent pas sur la valeur d'un bien, une menace ou une vulnérabilité, consigner le différend et calculer le risque résiduel à l'aide des deux valeurs.
- Pour gagner du temps et économiser des efforts, réutiliser les données des rapports d'EMR antérieurs, lorsque c'est possible.
- Une EMR non officielle est particulièrement utile pour déterminer si les éléments des évaluations antérieures peuvent être réutilisés pour des biens comparables dans des circonstances similaires.
- Il faut toujours respecter les normes de sécurité obligatoires. Si d'autres normes de sécurité sont disponibles et applicables, il convient de les employer de préférence à une EMR officielle.
- Comme il est expliqué à l'appendice A-2, une EMR non officielle est généralement nécessaire pour déterminer si ces normes sont entièrement applicables dans une situation particulière.
- Préparer un rapport final d'EMR le plus court possible.

[3] Voir la rubrique Introduction, à la page 2.

- Consigner uniquement les biens de plus grande valeur, les menaces les plus importantes, les vulnérabilités les plus graves et les risques résiduels inacceptables dans le corps du document; les détails doivent être présentés dans les annexes et les tables à l'appui.
- Se servir des notes en bas de page pour expliquer les motifs à l'appui d'une valeur d'un bien ou de l'importance d'une menace ou d'une vulnérabilité qui n'est pas explicite.

4 Feuille de travail EMR

L'appendice G-1 propose une feuille de travail EMR simple comme aide-mémoire utile aux spécialistes de la sécurité. Ce document de quatre pages dresse la liste de tous les processus et activités connexes pour chaque phase successive d'un projet d'EMR, et contient des renvois aux annexes et appendices pertinents. Cette feuille de travail contient également une version abrégée du tableau des préjudices, ainsi que des paramètres des menaces et des vulnérabilités. Ainsi, avec la pratique, un analyste chevronné de l'EMR peut produire un rapport d'EMR complet en consultant cette liste de vérification et en inscrivant les données pertinentes dans les tableaux visées, c'est-à-dire l'énoncé de sensibilité (appendice B-5), le tableau d'évaluation des menaces (appendice C-4) et le tableau d'évaluation des vulnérabilités (appendice D-4).

5 Sensibilité des rapports d'EMR

5.1 Généralités

En règle générale, la plupart des rapports d'EMR sont sensibles à une divulgation non autorisée, puisqu'ils définissent des vulnérabilités qui pourraient être exploitées pour compromettre les biens de valeur. Les préoccupations concernant la disponibilité sont généralement moins importantes, malgré les coûts associés au remplacement d'une évaluation perdue. Au contraire, une modification non autorisée des constatations pourrait entraîner de graves préjudices si l'analyse était par la suite mal interprétée et servait à recommander des mesures de protection inappropriées ou inadéquates. Les rapports d'EMR doivent donc être systématiquement classifiés afin d'identifier les valeurs de confidentialité, de disponibilité et d'intégrité conformément à la *Norme opérationnelle de sécurité sur l'identification des biens* et aux tests de préjudice expliqués à la section 3 de l'annexe B et détaillés à l'appendice B-4.

5.2 Valeur de confidentialité

En principe, les valeurs de confidentialité doivent être attribuées en fonction de l'importance des préjudices auxquels on peut raisonnablement s'attendre en cas de divulgation non autorisée. Du point de vue pratique, toutefois, il y a deux facteurs importants à prendre en considération :

- **Sources d'information.** Souvent, les données recueillies à l'occasion d'un projet d'EMR comprennent de l'information classifiée ou protégée, notamment celles qui sont colligées dans le cadre de la phase d'évaluation des menaces. À moins que le

document ne puisse être expurgé ou déclassé, le rapport final d'EMR doit être classifié et marqué comme il se doit.

- **Possibilité d'abus.** Même les rapports qui ne contiennent pas d'information classifiée ou protégée peuvent exiger d'être classifiés et protégés pour en préserver la confidentialité, parce que les vulnérabilités recensées durant la quatrième phase du projet d'EMR pourraient favoriser les menaces à l'égard de la disponibilité ou de l'intégrité, ce qui mènerait à la destruction, à la suppression, à la modification, à l'interruption d'accès ou à l'utilisation non autorisées des biens. Dans cette éventualité, la gravité des préjudices probables doit être déterminée en fonction du tableau détaillé des préjudices de l'appendice B-4. Le rapport d'EMR final doit ensuite être considéré comme classifié ou protégé au même niveau, selon que le préjudice a des répercussions à l'échelle nationale ou sur d'autres intérêts, et être marqué en conséquence.

5.3 Valeur de disponibilité

Un rapport d'EMR perdu ou détruit devra vraisemblablement être remplacé. Par conséquent, la mesure de la valeur de disponibilité la plus simple correspond au coût estimatif de la reconstitution du document en fonction des salaires et des dépenses connexes. Ce montant doit être comparé à celui qui figure dans la colonne Répercussion financière du tableau détaillé des préjudices pour déterminer la valeur de disponibilité appropriée, qui se trouve généralement dans la gamme Faible ou Moyenne. Dans quelques cas, toutefois, le rapport d'EMR peut être absolument nécessaire à des fins opérationnelles immédiates, par exemple pour le déploiement imminent de troupes dans un théâtre d'opérations à l'étranger. Dans une telle situation, le délai nécessaire à la reconstitution de l'évaluation initiale peut avoir des conséquences beaucoup plus graves, notamment la perte de vies; on doit alors attribuer au document une valeur de disponibilité supérieure, en fonction des préjudices possibles.

5.4 Valeur d'intégrité

La modification non autorisée d'un rapport d'EMR peut entraver l'ensemble du processus d'analyse, ce qui risque de mener à la formulation de recommandations inappropriées ou incomplètes et de mettre ainsi en péril les employés, les biens et la prestation des services. Compte tenu des conséquences potentielles, la valeur d'intégrité de la plupart des rapports d'EMR doit être aussi élevée que le préjudice le plus grave pouvant découler de la compromission de la confidentialité, de la disponibilité ou de l'intégrité des biens inclus dans la portée de l'évaluation, quelle qu'en soit la cause. Par exemple, dans le cas d'un projet d'EMR comportant de l'information Très secret et ayant, par conséquent, une valeur de confidentialité très élevée, la valeur d'intégrité du rapport final doit également être cotée très élevée, puisque la modification délibérée ou même accidentelle de son contenu pourrait exposer les données sensibles à une divulgation non autorisée.

6 Glossaire et acronymes

Un vocabulaire commun et cohérent de la gestion des risques est essentiel à l'amélioration des communications entre les spécialistes de la sécurité et à l'interopérabilité entre les projets d'EMR interdépendants, particulièrement lorsque de l'information et des biens partagés entrent en jeu. À cette fin, tous les termes techniques et les acronymes employés dans le texte de la *Méthodologie harmonisée d'EMR* sont définis à l'appendice G-2; la source est précisée, le cas échéant.

7 Références

Beaucoup de politiques et d'autres documents connexes sont cités dans la *Méthodologie harmonisée d'EMR*. Pour faciliter les renvois et les recherches, tous les documents cités sont énumérés à l'appendice G-3, sous les catégories générales suivantes :

- Politiques du Conseil du Trésor et publications connexes
- PGS : Normes opérationnelles de sécurité
- PGS : Documentation technique –
  - Publications du CST
  - Avertissements du MAECI
  - Publications de SPPCC
  - Publications de TPSGC
  - Publications de la GRC

Dans la mesure du possible, l'adresse URI (de l'anglais *Uniform Resource Identifier*) est fournie pour faciliter la consultation des documents dans Internet ou dans Publiservice, l'intranet du gouvernement du Canada.

Page intentionnellement laissée en blanc

Appendice G-1 – Feuille de travail EMR

Phase – Processus – Activité d'EMR	Référence	Page n°
Phase de préparation		
• Établir le mandat du projet d'EMR	• Annexe A, Section 3	A-4
• Déterminer la portée de l'évaluation	• Annexe A, Section 4	A-4
o Facteurs de planification	o Section 4.2	A-5
▪ Objet de l'évaluation	▪ Section 4.2.2	A-5
▪ Stade de développement	▪ Section 4.2.3	A-7
▪ Environnement de risque	▪ Section 4.2.4	A-7
▪ Quelques considérations pratiques	▪ Section 4.2.5	A-8
• Choisir l'équipe d'EMR	• Annexe A, Section 5	A-9
o Taille de l'équipe	o Section 5.2	A-9
o Qualifications des membres de l'équipe	o Section 5.3	A-10
o Membres de l'équipe de base	o Section 5.4	A-11
o Autres ressources	o Section 5.5	A-13
• Produire une ébauche du plan de travail de l'EMR	• Annexe A, Section 6 (Appendice A-6)	A-14
Phase d'identification et d'évaluation des biens		
• Identifier les biens inclus dans la portée de l'évaluation	• Annexe B, Section 2 (Appendice B-1)	B-2
o Biens corporels	o Section 2.2	B-2
o Biens incorporels	o Section 2.3	B-2
o Personnel	o Section 2.4	B-3
o Services	o Section 2.5	B-3
o Liste des biens	o Section 2.9 (Appendice B-2)	B-5
• Évaluer les préjudices	• Annexe B, Section 3	B-7
o Tableau des préjudices (Tableau 1 ci-dessous)	o Section 3.3 (Appendice B-4)	B-9
• Évaluer les biens	• Annexe B, Section 4	B-11
o Application pratique	o Section 4.2	B-12
▪ Confidentialité	▪ Section 4.2.2	B-12
▪ Disponibilité	▪ Section 4.2.3	B-12
▪ Intégrité	▪ Section 4.2.4	B-13
▪ Valeurs multiples	▪ Section 4.2.6	B-14
o Autres questions	o Section 4.3	B-14
▪ Valeurs variables des biens	▪ Section 4.3.2	B-14
▪ Regroupement et inférence	▪ Section 4.3.3	B-14
▪ Conventions d'évaluation des biens	▪ Section 4.3.4	B-15
• Compiler le tableau d'évaluation des biens/énoncé de sensibilité	• Annexe B, Section 5 (Appendice B-5)	B-17
Phase d'évaluation des menaces		
• Identifier les menaces	• Annexe C, Section 2	C-1
o Classes de menaces	o Section 2.2	C-2
▪ Menaces délibérées	▪ Section 2.2.2	C-2
▪ Menaces accidentelles	▪ Section 2.2.3	C-2
▪ Risques naturels	▪ Section 2.2.4	C-2
o Sources des données sur les menaces	o Section 2.3 (Appendice C-1)	C-3
o Techniques de collecte des données	o Section 2.4	C-3
o Liste des menaces	o Section 2.5 (Appendice C-2)	C-4
• Évaluer la probabilité d'occurrence (Tableau 2 ci-dessous)	• Annexe C, Section 3 (Appendice C-3)	C-12
• Évaluer la gravité (Tableau 3 ci-dessous)	• Annexe C, Section 4 (Appendice C-3)	C-15
• Attribuer les niveaux de menaces (Tableau 4 ci-dessous)	• Annexe C, Section 5 (Appendice C-3)	

Phase – Processus – Activité d'EMR	Référence	Page n°
• Compiler le tableau priorisé d'évaluation des menaces	• Annexe C, Section 6 (Appendice C-4)	C-17 C-19
Phase d'évaluation des risques – Évaluation des vulnérabilités		
• Recenser les mesures de protection existantes ou proposées • Évaluer leur efficacité	• Annexe D, Section 2	D-1
• Identifier les autres vulnérabilités o Sources de données sur les vulnérabilités o Techniques de collecte des données o Liste des vulnérabilités	• Annexe D, Section 3 • Annexe D, Section 4	D-2 D-6 D-11 D-12
• Analyser leur incidence o Probabilité de compromission (Tableau 5 ci-dessous) o Gravité des conséquences (Tableau 6 ci-dessous)	o Section 4.3 (Appendice D-1) o Section 4.4 o Section 4.5 (Appendice D-2) • Annexe D, Section 5 (Appendice D-3)	D-13 D-14 D-14
• Attribuer les niveaux de vulnérabilité (Tableau 7 ci-dessous)	o Section 5.2 o Section 5.3 • Annexe D, Section 6	D-17 D-19
• Compiler le tableau priorisé des vulnérabilités	• Annexe D, Section 7 (Appendice D-4)	D-22
Phase d'évaluation des risques – Calcul des risques résiduels		
• Calculer les risques résiduels o Calcul de base des risques (Tableau 8 ci-dessous) o Niveaux de risque (Tableau 9 ci-dessous)	• Annexe E, Section 2 o Section 2.2 o Section 2.3 (Appendice E-1)	E-1 E-1 E-2
• Compiler la liste priorisée des risques résiduels évalués	• Annexe E, Section 3 (Appendice E-2)	E-4
Phase de recommandations		
• Identifier les risques résiduels inacceptables o Gammes de risques (Tableau 9 ci-dessous)	• Annexe F, Section 2 o Section 2.3	F-1 F-2
• Sélectionner les mesures de protection potentielles o Efficacité des mesures de protection	• Annexe F, Section 3 (Appendice F-2) o Section 3.3 (Appendice F-3)	F-4 F-6
• Identifier les coûts o Coûts directs o Coûts ou avantages indirects o Rentabilité	• Annexe F, Section 4 o Section 4.2 o Section 4.3 o Section 4.4 (Appendice F-4)	F-10 F-10 F-11 F-12
• Évaluer les risques résiduels projetés	• Annexe F, Section 5 (Appendice F-5)	F-14
• Préparer le rapport final d'EMR	• Annexe F, Section 6 (Appendice F-6)	F-14

Phase d'identification et d'évaluation des biens

Tableau 1 : Tableau détaillé des préjudices

Niveau de préjudice	Préjudices aux personnes		Répercussions financières
	Préjudice physique	Préjudice psychologique	
Très élevé	Pertes de vies massives	Traumatisme généralisé	> 1 G$
Élevé	Pertes de vie potentielles	Stress/traumatisme grave	> 10 M$
Moyen	Blessures/maladies	Méfiance/doutes du public	> 100 K$
Faible	Inconfort	Léger embarras	> 1 K$
Très faible	Négligeable	Négligeable	< 1 K$

Phase d'évaluation des menaces

Tableau 2 : Tableau de la probabilité des menaces			
Fréquence antérieure	**Même endroit, biens semblables**	**Endroit distant mais biens semblables ou Même endroit mais biens différents**	**Endroit distant, autres biens**
Quotidienne	Élevée	Élevée	Élevée
1-10 jours	Élevée	Élevée	Moyenne
10-100 jours	Élevée	Moyenne	Faible
100-1 000 jours	Moyenne	Faible	Très faible
1 000-10 000 jours	Faible	Très faible	Très faible
Plus de 10 000 jours	Très faible	Très faible	Très faible

Phase d'évaluation des menaces (suite)

Tableau 3 : Tableau de la gravité des menaces		
Capacités de l'agent de menace délibérée	**Magnitude des accidents ou des risques naturels**	**Incidence ou gravité de la menace**
Connaissances/compétences étendues et ressources importantes	Hautement destructifs Erreur extrêmement grave Utilisation abusive généralisée	Élevée
Connaissances/compétences limitées et ressources importantes **ou** Connaissances/compétences étendues et ressources limitées **ou** Connaissances et compétences modérées et ressources moyennes	Modérément destructifs Erreur grave Utilisation abusive importante	Moyenne
Connaissances/compétences limitées et ressources limitées	Peu destructifs Erreur mineure Utilisation abusive limitée	Faible

Tableau 4 : Tableau des niveaux de menace				
Incidence de la menace	**Probabilité de la menace**			
	Très faible	**Faible**	**Moyenne**	**Élevée**
Élevée	Faible	Moyenne	Élevée	Très élevée
Moyenne	Très faible	Faible	Moyenne	Élevée
Faible	Très faible	Très faible	Faible	Moyenne

Phase d'évaluation des risques – Évaluation des vulnérabilités

Tableau 5 : Incidence des vulnérabilités sur la probabilité de compromission (prévention)		
Efficacité des mesures de protection	**Vulnérabilités connexes**	**Probabilité de compromission**
Aucune mesure de protection Mesure inefficace en grande partie Probabilité de compromission > 75 %	Facilement exploitables Besoin de peu de connaissances/ compétences/ressources Biens hautement accessibles Biens très complexes/fragiles/portables Employés mal informés/formés	Élevée
Mesure modérément efficace Probabilité de compromission 25-75 %	Pas facilement exploitables Besoin de certaines connaissances/ compétences/ressources Biens modérément accessibles Biens modérément complexes/fragiles/portables Employés modérément informés/formés	Moyenne
Mesure très efficace Probabilité de compromission < 25 % (Mesure remplissant uniquement des fonctions de détection, de réaction ou de reprise)	Difficiles à exploiter Besoin de très bonnes connaissances/ compétences/ressources Accès aux biens rigoureusement contrôlé Biens très simples/robustes/statiques Employés bien informés/formés	Faible (Sans objet)

Phase d'évaluation des risques – Évaluation des vulnérabilités (suite)

Tableau 6 : Incidence des vulnérabilités sur la gravité des conséquences (détection, réaction ou reprise)		
Efficacité des mesures de protection	**Vulnérabilités connexes**	**Gravité des conséquences**
Aucune mesure de protection Mesure en grande partie inefficace Biens exposés à des préjudices importants	Détection improbable des compromissions Dommages difficiles à contenir Délais de reprise prolongés/Niveaux de service faibles Biens très complexes/fragiles Employés mal informés/formés	Élevée
Mesure modérément efficace Biens exposés à des préjudices modérés	Compromissions probablement détectées au fil du temps Dommages partiellement contenus Délais de reprise/Niveaux de service modérés Biens relativement complexes/fragiles Employés modérément informés/formés	Moyenne
Mesure très efficace Biens exposés à des préjudices légers (Mesures de protection ayant pour seule fonction la prévention)	Compromissions presque certainement détectées rapidement Dommages rigoureusement contenus Reprise rapide et complète Biens très simples/robustes Employés bien informés/formés	Faible (Sans objet)

Tableau 7 : Évaluation des vulnérabilités			
Incidence sur la gravité des conséquences (détection, réaction et reprise)	**Prévention (probabilité de compromission)**		
	Faible (s. o.)	**Moyenne**	**Élevée**
Élevée	Moyenne	Élevée	Très élevée
Moyenne	Faible	Moyenne	Élevée
Faible	Très faible	Faible	Moyenne

Phase d'évaluation des risques – Calcul du risque résiduel

Tableau 8 : Cotes numériques – Valeur du bien, menace et niveaux de vulnérabilité					
Niveau de la valeur du bien, des menaces et des vulnérabilités	Très faible	Faible	Moyen	Élevé	Très élevé
Cote de calcul du risque	1	2	3	4	5

Tableau 9 : Niveaux et gammes de risques					
Note de base du risque	1-4	5-12	15-32	36-75	80-125
Niveau de risque	Très faible	Faible	Moyen	Élevé	Très élevé
Nombre de résultats dans la gamme	13	34	43	28	7
Acceptabilité du risque	Tout à fait acceptable	Probablement acceptable	Peut-être acceptable	Probablement inacceptable	Tout à fait inacceptable

Nota :

1. La feuille de travail d'EMR inclut la liste de toutes les activités et processus successifs de chaque phase d'un projet d'EMR.
2. Les copies de tous les tableaux requis pour évaluer les niveaux des valeurs des biens, des menaces et des vulnérabilités, ainsi que les risques résiduels, sont inclues dans le même ordre logique pour en faciliter l'utilisation.
3. Cette feuille de travail, qui inclut des copies du tableau d'évaluation des biens/énoncé de sensibilité (appendice B-5), du tableau d'évaluation des menaces (appendice C-4), du tableau d'évaluation des vulnérabilités (appendice D-4), de la liste des risques résiduels évalués (appendice E-2) et du tableau des recommandations (appendice F-5), constitue la trousse d'outils de base pour effectuer une EMR.

Page intentionnellement laissée en blanc

Appendice G-2 – Glossaire et acronymes

1 Préface

Les termes et acronymes définis dans l'appendice G-2, Glossaire et acronymes, sont utilisés dans la *Méthodologie harmonisée de l'évaluation des menaces et des risques*. La plupart proviennent de la *Politique du gouvernement sur la sécurité* (PGS) et des documents connexes. Dans certains cas, toutefois, certaines définitions ont été élargies aux fins de clarté, d'uniformité ou d'intégralité. Dans ce cas, les deux définitions, l'ancienne et la nouvelle sont incluses aux fins de comparaison. Enfin, certaines définitions ont été formulées pour décrire des concepts ou processus précis de la méthodologie.

2 Sources

Lorsqu'un terme a été précédemment défini, sa source est indiquée. Toute nouvelle définition est clairement est indiquée en tant que telle. Les sources possibles sont les suivantes :

[GPS]..... *Politique du gouvernement sur la sécurité*
[IB].....*Norme opérationnelle de sécurité– Identification des biens* (ébauche)
[NSM] ..... *Norme opérationnelle sur la sécurité matérielle*
[Nouv] ..... *Groupe de travail sur la méthodologie harmonisée d'EMR*

3 Navigation

Des hyperliens ont été utilisés dans le glossaire pour en faciliter la navigation. Appuyez sur CTRL et cliquez sur une lettre de l'alphabet pour visualiser les termes commençant par cette lettre. Les icônes de lettre dans le corps du texte comprennent un lien « Début » qui ramène le curseur à la ligne de navigation.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A Home

AAE *(EAA)* – Autorisation et authentification électroniques.

Accès non autorisé *(unauthorized access)* – **[NSM]** – Accès à des biens par un particulier qui n'a pas fait l'objet d'une enquête de sécurité du personnel exigée ou ne satisfait pas aux critères du besoin de connaître, ou les deux.

Accréditation *(accreditation)* **– [PGS]** – autorisation officielle par la direction d'exploiter un système des TI et acceptation par la direction du risque résiduel s'y rattachant. L'accréditation dépend des résultats de la certification ainsi que d'autres considérations de nature administrative.

AIPRP *(ATIP)* **–**Accès à l'information et protection des renseignements personnels.

ARO *(BIA)* **–** Analyse des répercussions sur les opérations.

ASIS **–** American Society for Industrial Security.

ASM *(DSO)* **–** Agent de sécurité du ministère.

Attaque subreptice *(surreptitious attack)* **– [NSM]** – Attaque secrète et non autorisée visant à percer ou contourner un système de protection ou certaines de ses composantes de manière à ce que les gardiens ou la force d'intervention ne puissent la détecter facilement.

B Home

Besoin de connaître *(need-to-know)* **– [PGS]** – Besoin éprouvé par une personne d'accéder à des renseignements et de les connaître pour accomplir les tâches qui lui incombent.

Biens *(assets)* **– [PGS]** – Éléments d'actifs corporels ou incorporels du Gouvernement du Canada. Ce terme s'applique, sans toutefois s'y limiter, aux renseignements, sous toutes leurs formes et quel que soit leur support, aux réseaux, aux systèmes, au matériel, aux biens immobiliers, aux ressources financières, à la confiance des employés et du public, et à la réputation internationale.

Biens classifiés *(classified assets)* – **[PGS]** - Biens dont la divulgation sans autorisation risquerait vraisemblablement de porter préjudice à l'intérêt national.

Biens essentiels *(critical assets)* – **[PGS]** - Biens supportant un service essentiel.

Biens protégés *(protected assets)* **– [NSM]** – Biens dont la divulgation sans autorisation risquerait vraisemblablement de porter préjudice à des intérêts privés ou non reliés à l'intérêt national.

C Home

CERT/CC **–** Computer Emergency Response Team/Coordination Center, Carnegie Mellon University.

Certification *(certification)* – **[PGS]** - Évaluation complète des dispositifs de sécurité techniques et non techniques d'un système des TI et d'autres mesures de sauvegarde connexes, effectuée à l'appui de l'accréditation, pour déterminer le degré selon lequel un modèle de conception et de mise en œuvre précis satisfait à un ensemble donné d'exigences en matière de sécurité.

Compromission *(compromise)* – **[PGS] -** Divulgation, destruction, suppression, modification, interruption d'accès ou utilisation de biens qui est non autorisée.

Confidentialité *(confidentiality)* – **[PGS]** - Caractéristique selon laquelle les renseignements ne doivent pas être divulgués à des personnes non autorisées, cela pouvant porter préjudice à l'intérêt national ou à d'autres intérêts, comme l'indiquent des dispositions précises de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*.

CPCA *(BCPC)* – Coordonnateur de la planification de la continuité des activités.

Csis, Inc. – Canadian Society for Industrial Security, Inc.

CST *(CSE)* – Centre de la sécurité des télécommunications.

CSTI *(ITSC)* – Coordonnateur de la sécurité des technologies de l'information.

Destruction *(destruction)* – **[Nouv]** – Altération physique d'un bien ou blessure d'un employé qui peut empêcher ce bien ou cet employé d'exercer ses fonctions principales.

Détection *(detection)* – **[NSM]** – Utilisation des mécanismes, des systèmes et des procédures qui s'imposent pour signaler qu'il y a eu tentative d'accès non autorisé ou accès non autorisé.

Disponibilité *(availability)* – **[PGS]** - Condition d'être disponible sur demande afin de soutenir les opérations, les programmes et les services.

Divulgation non autorisée *(unauthorized disclosure)* – **[NSM]** – Divulgation interdite par la loi ou par des politiques gouvernementales ou ministérielles.

(EMR) Dossier *(record)* – **[Nouv]** – Rapport d'EMR accompagné de toute la documentation pertinente recueillie dans le cadre d'un projet d'EMR à l'appui des conclusions et recommandations finales.

DPI *(CIO)* – Dirigeant principal de l'information.

EFVP *(PIA)* **–** Évaluation des facteurs relatifs à la vie privée.

EMR *(TRA)* **–** Évaluation des menaces et des risques.

Exigences sécuritaires de base *(baseline security requirements)* **– [PGS], [NSM]** - Dispositions obligatoires de la Politique du gouvernement sur la sécurité, de ses normes opérationnelles et de sa documentation technique.

GI/TI *(IM/IT)* **–** Gestion de l'information/Technologies de l'information.

GRC *(RCMP)* **–** Gendarmerie royale du Canada.

HIS *(HIS)* **–** Service de renseignement ennemi.

Inférence *(inference)* **– [IB]** – Situation où l'analyse de biens catégorisés à un certain niveau de sensibilité permet de conclure qu'il existe un risque de préjudice plus élevé.

Installation *(facility)* **– [PGS]** – Désigne un aménagement physique qui sert à une fin précise. On entend par installation une partie ou la totalité d'un immeuble, soit un immeuble, son emplacement et ses alentours, ou encore une construction qui n'est pas un immeuble. Le terme désigne non seulement l'objet même mais aussi son usage.

Intégrité *(integrity)* **– [PGS]** – Exactitude et intégralité des biens, et authenticité des transactions.

Intérêt national *(national interest)* **– [NSM]** – Concerne la défense et le maintien de la stabilité sociopolitique et économique du Canada.

Interruption *(interruption)* **– [Nouv]** – Arrêt temporaire de la disponibilité d'employés, de biens ou de services.

Intervention *(response)* **– [NSM]** – Mise en oeuvre de mesures visant à faire en sorte que les incidents en matière de sécurité soient déclarés aux responsables en la matière et que des correctifs immédiats et à long terme soient adoptés.

MAECI *(DFAIT)* **–** Ministère des Affaires extérieures et du Commerce international.

Menace *(threat)* **– 1 [PGS]** – tout événement ou acte éventuel, délibéré ou accidentel, qui pourrait porter préjudice aux employés ou aux biens**; 2 [Nouv]** – tout événement ou acte éventuel, délibéré ou accidentel, ou risque naturel qui pourrait porter préjudice aux employés ou aux biens et ainsi avoir une incidence négative sur la prestation de services.

Menace accidentelle *(accidental threat)* **– [Nouv]** – Menace sans préméditation causée par une personne.

Menace délibérée *(deliberate threat)* **– [Nouv]** – Menace planifiée ou préméditée par une personne.

Mesures de protection *(safeguards)* **– [Nouv]** – Biens ou contrôles externes qui réduisent les risques globaux à l'égard des employés, d'autres biens ou de la prestation des services en abaissant la probabilité des incidents ou des compromissions ou en atténuant la gravité des conséquences par l'interaction directe ou indirecte avec les valeurs d'un bien, les menaces ou les vulnérabilités.

Ministère responsable en matière de sécurité *(lead security department)* **– [Nouv, basée sur la PGS]** – Ministère ou organisme ayant des responsabilités sur le plan de la sécurité à l'échelle du gouvernement, telles qu'elles ont été définies dans la PGS.

Modification *(modification)* **– [Nouv]** – Altération des données ou des capteurs ou systèmes qui traitent l'information, nuisant par le fait même à l'exactitude ou à l'intégralité des biens ou l'authenticité des transactions.

PCA *(BCP)* – Planification de la continuité des activités.

PDRR *(PDRR)* – Protection, détection, réaction et reprise ; la stratégie de défense active.

PGS *(GSP)* – *Politique du gouvernement sur la sécurité*.

(EMR) Phase *(phase)* – **[Nouv]** – L'un des cinq principaux segments d'un projet d'EMR, soit la préparation, l'identification et l'évaluation des biens, l'évaluation des menaces, l'évaluation des risques et les recommandations.

Planification de la continuité des activités*(business continuity planning)* – **[PGS]** - Terme global s'appliquant notamment à l'élaboration et à l'exécution opportune de plans, de mesures, de procédures et de préparatifs afin d'éviter ou de minimiser tout arrêt de la disponibilité des services et des biens essentiels.

Préjudice *(injury)* – **[IB]** – Dommage résultant de la compromission d'un bien.

(EMR) Processus *(process)* – **[Nouv]** – Activité principale réalisée dans le cadre de chaque phase d'un projet d'EMR.

(EMR) Projet *(project)* – **[Nouv]** –] Application des processus d'EMR à un sujet précis en vue de terminer un rapport d'EMR à partir d'un dossier d'EMR complet.

Protection *(protection)* – **[NSM]** – En matière de sécurité matérielle, « protection » désigne le recours à des obstacles matériels, psychologiques et de procédure visant à retarder l'accès non autorisé ou à exercer un effet dissuasif à cet égard, y compris les obstacles visuels et auditifs.

R et D *(R&D)* **–** Recherche et développement.

(EMR) Rapport *(report)* **– [Nouv]** – Document final d'un projet d'EMR, présenté au responsable de l'acceptation des risques aux fins d'examen et d'approbation par la direction.

Regroupement *(aggregation)* **– [IB]** – Situation où un ensemble de biens peuvent être catégorisés à un niveau de sensibilité plus élevé que les parties qu'il forme en raison du préjudice accru que pourrait causer toute compromission à ce bien. Le regroupement s'applique généralement à la confidentialité, mais, dans certains cas, il peut également s'appliquer à la disponibilité et à l'intégrité.

Renseignements *(information)* **– [NSM] -** Suite de symboles ou de sons auxquels un sens peut être attribué.

Renseignements classifiés *(classified information)* **– [PGS]** - Renseignements d'intérêt national susceptibles d'être visés par une exclusion ou une exception en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, et dont la divulgation sans autorisation risquerait vraisemblablement de porter préjudice à l'intérêt national.

Renseignements protégés *(protected information)* **– [PGS] –** Renseignements autres que d'intérêt national susceptibles d'être visés par une exclusion ou une exception en vertu de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels*, et dont la divulgation sans autorisation risquerait vraisemblablement de porter préjudice à des intérêts privés ou non reliés à l'intérêt national

Reprise *(recovery)* **– [NSM]** – Rétablissement du niveau intégral de prestation des services.

Responsable de l'acceptation des risques *(risk acceptance authority)* **– [Nouv]** – Cadre supérieur ayant les pouvoirs, les responsabilités et la reddition de comptes nécessaires pour examiner et approuver les recommandations formulées dans un rapport d'EMR.

RHDSC *(HRSDC)* **–** Ressources humaines et Développement social Canada.

Risque *(risk)* **– [PGS]** – Possibilité qu'une vulnérabilité soit exploitée.

Risque naturel *(natural hazard)* **– [Nouv]** – Menace attribuable aux forces de la nature.

Risque résiduel *(residual risk)* **– [Nouv]** – Portion du risque qui demeure une fois que les mesures de sécurité visant à le réduire ont été sélectionnées et mises en œuvre.

Risque résiduel accepté *(accepted residual risk)* **– [Nouv]** – Niveau de risque approuvé par le responsable de l'acceptation des risques, généralement en fonction des recommandations finales formulées dans un rapport d'EMR.

Risque résiduel évalué *(assessed residual risk)* **– [Nouv]** – Risque résiduel calculé durant la phase d'évaluation des risques d'un projet d'évaluation des menaces et des risques (EMR).

Risque résiduel projeté *(projected residual risk)* **– [Nouv]** – Risque résiduel obtenu par suite de la mise en œuvre de toutes les recommandations formulées dans le rapport d'EMR final.

S Home

SCRS *(CSIS)* **–** Service canadien du renseignement de sécurité.

Sécurité des technologies de l'information *(information technology security)* **– [PGS]** – Mesures de protection visant à préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique.

Sécurité matérielle *(physical security)* **– [PGS]** - mesures de sauvegarde matérielle pour empêcher ou retarder l'accès non autorisé aux biens, pour détecter l'accès non autorisé recherché et obtenu et pour déclencher une intervention appropriée.

Service essentiel *(critical service)* **– [PGS]** - Service dont la compromission en termes de disponibilité ou d'intégrité résulterait en un préjudice élevé à la santé, la sûreté, la sécurité et le bien-être économique des Canadiens et des Canadiennes ou encore à l'efficacité du Gouvernement du Canada.

SPPCC *(PSEPC)* – Sécurité publique et Protection civile Canada.

SST *(OSH)* **–** Santé et sécurité au travail.

T Home

TPSGC *(PWGSC)* – Travaux publics et Services gouvernementaux Canada.

U Home

V Home

Valeur *(value)* **– [PGS]** – Coût approximatif soit monétaire, culturel ou autre.

Valeur monétaire *(dollar value)* **– [Nouv]** – Valeur appréciée ou dépréciée de biens corporels; coût de remplacement.

Vulnérabilité *(vulnerability)* **– 1 [GPS]** – Faiblesse quant à la sécurité qui pourrait permettre à une menace de causer préjudice; **2 [Nouv]** – Attribut d'un bien, ou de l'environnement dans lequel il se trouve, qui augmente la probabilité d'un incident, la probabilité de compromission ou la gravité des conséquences. Les vulnérabilités sont inversement proportionnelles à l'efficacité des mesures de protection.

Zones *(zones)* **– [NSM]** – Une série d'espaces clairement visibles pour contrôler progressivement l'accès.

Page intentionnellement laissée en blanc

Appendice G-3 – Documents de référence

1 Politiques du Conseil du Trésor et autres publications connexes

Cadre de gestion intégrée du risque, avril 2001.
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_f.asp

Cadre de responsabilisation de gestion du SCT, 2003.
http://www.tbs-sct.gc.ca/maf-crg/documents/booklet-livret/booklet-livret_f.asp

Des résultats pour les Canadiens et les Canadiennes : Un cadre de gestion pour le gouvernement du Canada, mars 2001.
http://www.tbs-sct.gc.ca/report/res_can/siglist_f.asp

Lignes directrices sur l'évaluation des facteurs relatifs à la vie privée – Cadre de gestion des risques d'entrave à la vie privée, août 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_f.asp

Politique d'évaluation des facteurs relatifs à la vie privée, mai 2002.
http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr_f.asp

Politique du gouvernement sur la sécurité, février 2002.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_f.asp

Politique sur la gestion des risques, avril 1994.
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/riskmanagpol_f.asp

Protection des renseignements personnels, décembre 1993.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1_f.asp

Rapport du Groupe de travail indépendant chargé de la modernisation de la fonction de contrôleur dans l'Administration fédérale du Canada, octobre 1997.
http://www.tbs-sct.gc.ca/cmo_mfc/resources2/review_panel/rirp06_f.asp

2 PGS : Normes opérationnelles de sécurité

Enquêtes de sécurité et sanctions, ébauche, le 28 mai 2005.

Filtrage de sécurité, ébauche, le 30 avril 2004.

Formation et sensibilisation à la sécurité, version provisoire, le 15 mars 2005.
http://publiservice.tbs-sct.gc.ca/gs-sg/spins/2005/2005-05-spin_f.asp

Gestion de la sécurité des technologies de l'information, avril 2004.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_f.asp

Gestion des risques liés à la sécurité, ébauche, le 1er mai 2005.

Identification des biens, ébauche, le 9 février 2005.
http://publiservice.tbs-sct.gc.ca/gos-sog/gs-sg/spins/2005/2005-03_f.asp

Niveaux de préparation des installations du gouvernement fédéral, le 1er novembre 2002.
http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/oss-nos_f.asp

Programme de planification de la continuité des activités (PCA), mars 2004.
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/ossbcp-nsopca_f.asp

Sécurité dans la gestion des marchés, version provisoire, le 24 mars 2005.
http://publiservice.tbs-sct.gc.ca/gs-sg/spins/2005/2005-06-spin_f.asp

3 PGS : Documentation technique

3.1 Publications du CST

ITSA-09 – *Élimination du matériel COMSEC*, le 15 janvier 1998.
http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsa/itsa09-f.pdf

ITSA-10 – *Signalement des incidents COMSEC*, le 1er décembre 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsa/itsa10-f.html

ITSB-02 – *Évaluation de la vulnérabilité des systèmes de communication sans fil du gouvernement du Canada*, août 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb02-f.html

ITSB-03 – *Tendances en matière de technologies sans fil et de sécurité des appareils sans fil*, le 30 octobre 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb03-f.html

ITSB-06 – *Le CST approuve le BlackBerry sécurisé,* le 6 mai 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb06-f.html

ITSB-09 - *Fonctionnement du STU-III pendant une panne d'électricité*, le 10 octobre 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb09-f.html

ITSB-12 – *Acquisition du module de sécurité Blackberry*, le 29 octobre 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb12-f.html

ITSB-13 – *Commande de clés pour les STE*, le 28 octobre 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb13-f.html

ITSB-15 – *Vulnérabilité sur le plan de la sécurité présentée par les ordinateurs portatifs équipés de la technologie WLAN*, le 11 février 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb15-f.html

ITSB-18 – *Liste des produits recommandés par l'OTAN (NRPL) – produits TEMPEST homologués*, le 5 mai 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb18-f.html

ITSB-19 – *Mesures de sécurité – appareils électroniques sans fil*, le 19 mai 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsb/itsb19-f.html

ITSB-29 – *Offre à commandes concernant le module de sécurité GSM (Global System for Mobile Communication) SECTERA (SGSM)*, le 1er mai 2006.
http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsb/itsb29-f.pdf

ITSD-01 – *Directives sur l'application de la sécurité des communications au sein du gouvernement du Canada*, janvier 2005.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsd/itsd01-f.html

ITSD-02 – *Exigences sécuritaires de base en matière de zones de sécurité TI*, mai 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsd/itsd02-f.html

ITSG-06 – *Effacement et déclassification des supports d'information électroniques*, août 2000.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg06-f.html

ITSG-10 – *Manuel de contrôle du matériel COMSEC*, janvier 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg10-f.html

ITSG-13 –*Manuel sur la commande de clés cryptographiques*, mai 2006.
http://www.cse-cst.gc.ca/documents/publications/gov-pubs/itsg/itsg13-f.pdf

ITSG-20 – *Sécurité de base recommandée pour Windows Server 2003*, mars 2004.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/itsg20-f.html

ITSPSR-14 – *Projet de télétravail*, mars 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr14-f.html

ITSPSR-16 – *Évaluation de la vulnérabilité des Services de communications personnelles (SCP) et des systèmes cellulaires*, octobre 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr16-f.html

ITSPSR-17 – *Évaluation des vulnérabilités de Bluetooth*, octobre 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr17-f.html

ITSPSR-18 – *Évaluation des vulnérabilités des assistants numériques personnels (PDA)*, octobre 2002.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr18-f.html

ITSPSR-19 – *Sécurité de base recommandée pour Windows 2000 Pro et X Pro*, mai 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr19-f.html

ITSPSR-21 – Évaluation de la vulnérabilité des réseaux locaux (LAN) sans fils 802.11, mai 2003.
http://www.cse-cst.gc.ca/publications/gov-pubs/itspsr/itspsr21-f.html

MG-1 – *Sécurité des réseaux, analyse et mise en oeuvre*, janvier 1996.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg1-f.html

MG-2 – *Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information,* janvier 1996.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg2-f.html

MG-4 – *Guide de certification et d'accréditation des technologies de l'information*, janvier 1996.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg4-f.html

MG-9 – *Manuel canadien de la sécurité des technologies de l'information*, mars 1998.
http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg9-f.html

3.2 Avertissements du MAECI en matière de voyage

Avertissements (Affaires consulaires)
http://www.voyage.gc.ca/dest/sos/warnings-fr.asp

3.3 Publications de SPPCC

Programme de planification de la continuité des activités, le 4 mars 2004.
http://rcmp-grc.gc.ca/tsb-genet/awareness/2004-PSEPC-BCP-fr.doc

3.4 Publications de TPSGC

Manuel de la sécurité industrielle, mai 2006.
http://www.ciisd.gc.ca/text/ism/toc-f.asp

3.5 Publications de la GRC

G1-001 – *Guide d'équipement de sécurité*
http://www.rcmp-grc.gc.ca/tsb-genet/seg/html/home_f.htm

G1-002 – *Éclairage de sécurité*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-003 – *Vitrage*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-004 - *Construction d'une aire protégée*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-005 – *Guide pour la préparation d'un énoncé de sécurité matérielle*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-006 – *Cartes d'identité / Insignes d'accès*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-007 – *Scellage de protection des clés d'urgence et passe-partout ou des serrures à code d'immeubles*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-008 – *Lignes directrices visant les services de gardiens*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-009 –*Transport et transmission de renseignements protégés ou classifiés*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-010 – *Éléments du Code national du bâtiment 1995 touchant la sécurité*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-011 – *Devis de construction de portes escamotables en plafond*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-013 – *Besoins en espace des centres de surveillance*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-014 – *Devis de construction d'une barrière pour échelle extérieure*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-015 – *Contrôle des accès, portes basculantes*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-016 – *Les systèmes de clés maîtresses*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-017 – *Quincaillerie*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-018 – *Portes et cadres de portes*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-019 – *Chambres fortes*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-024 – *Contrôle de l'accès*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-025 – *Protection, détection et intervention*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-026 – *Établissement des zones de sécurité matérielle*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-027 – *Responsabilités des ministères gardiens et des ministères locataires en matière de sécurité matérielle*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-029 – *Pièces sécuritaires*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G1-030 – *Guide de sensibilisation à la sécurité*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/g1-030_f.htm

G1-031 – *Pièces pour serveurs*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/phys_sec/index_f.htm

G2-002 – *Guide sur la répression des vols de matériel informatique*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

G2-003 – *Lignes directrices sur l'élimination et la destruction des renseignements protégés sur disques durs*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

G2-004 – *Guide de configuration de sécurité avancée pour Windows 2000 Professional*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

G2-005 – *Guide de configuration de sécurité du Active Directory de Windows 2000*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

B2-001 – *Produits de remplacement pour DSX*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

R2-001 – *Les technologies biométriques : une évaluation d'applications pratiques*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

R2-002 – *Logiciels malveillant : les tendances qui se dessinent*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

DSX-G – *Manuel de l'utilisateur pour le logiciel de réécriture de disque dur (DSX) de la GRC*
http://www.rcmp-grc.gc.ca/tsb-genet/pubs/it_sec/index_f.htm

Page intentionnellement laissée en blanc